TUTTI I SOFTWARE MIGLIORI SPIEGATI PASSO PASSO

HACKERS

MAGAZINE.IT

HACKERARE KINECT

Le modifiche più incredibili per la periferica Xbox

WINDOWS A MODO TUO

I trucchi migliori per mettere mano al registro

DEFCON 2011

All'assalto di Android

HACKERS MAGAZINE N°69 - BIM. - ANNO 10 - 2011
€ 4,99 - DISTRIBUTORE: M-DIS DISTRIBUZIONE SPA
10069
9 771720 767009
WLF PUBLISHING

HACKING
MULTIMEDIA
PROGRAMMING
COPY
NETWORKING
SYSTEM
WEB
P2P
SECURITY

SOMMARIO

STRUMENTI ESSENZIALI

Questo numero è in parte dedicato a una serie di strumenti essenziali che non devono mancare nell'arsenale di nessun hacker. Alcuni di questi sono già noti a chi smanetta seriamente sul Web: Firebug è infatti il coltellino svizzero per la modifica del codice delle pagine HTML e non solo. Altri, come YouTube Downloader, offrono incredibili potenzialità sfruttando sistemi già noti: è vero che scaricare i filmati di YouTube è facile e accessibile a tutti già da tempo ma questo programma permette di scaricare filmati da decine di siti Web, in tutti i formati che volete e con la possibilità di modificare parecchi parametri. Imperdibile!

Per chi invece usa spesso i database, PHPMyAdmin è uno strumento semplicemente fondamentale. Sostituisce completamente la linea di comando e mette nei programmatori tutta la potenza di MySQL senza però i mal di testa da digitazione delle query. Nella borsa degli attrezzi poi non possono naturalmente mancare sistemi di criptazione come Hallucinate e Secure Folder...

Infine, prosegue la rubrica Game Hack con una serie di modifiche a Kinect di Microsoft per Xbox da fare cadere la mascella: generazione di ambienti 3D, sistemi di controllo per i robot da pulizia, specchi magici e molto altro ancora...

Buona lettura!

La redazione

HACKERSMAGAZINE.IT
Bimestrale - 4,99 euro

Sprea International
Via Torino, 51 - Cernusco Sul Naviglio (MI) - Italy
Tel. (+39) 02.92.43.21
Fax (+39) 02.92.43.2.236

Direttore responsabile:
Luca Sprea - direttore@hackersmagazine.it

Redazione: redazione@hackersmagazine.it

Amministrazione: Anna Nese - amministrazione@sprea.it

Foreign Rights: Gabriella Re - international@sprea.it

Marketing: Walter Longo - marketing@sprea.it

Stampa: Arti Grafiche Boccia S.p.a. - Salerno
Carta: Valpaco Paper Supply Chain Optimizer
Distribuzione: M-Dis Distribuzione Spa
Via Cazzaniga, 19 – 20132 Milano

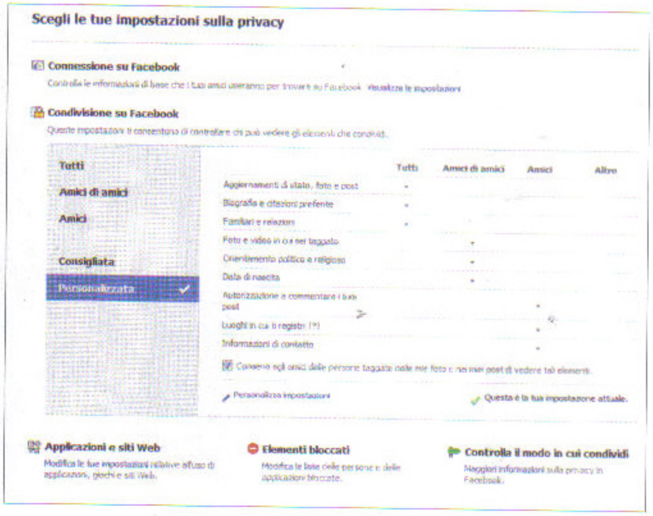
HACKERS MAGAZINE
Pubblicazione registrata al Tribunale di Milano il 15/07/2002 con il numero 414.

FINE DEL NOSTRO ANONIMATO?

IL BULLISMO SU INTERNET E IL CYBERTERRORISMO SONO COSE SERIE, MA LA SOLUZIONE È DAVVERO RINUNCIARE ALLA NOSTRA PRIVACY?

Randi è la Zuckerberg meno famosa, sorella del creatore di Facebook ed ex direttore del marketing per il social network più famoso. Recentemente ha commentato i fenomeni di bullismo sulla Rete dicendo che l'anonimato online dovrebbe essere combattuto e abolito. Facebook già richiede, a suo dire, nomi veri e e-mail valide (sappiamo tutti come questi vincoli vengano puntualmente aggirati) e in futuro i controlli dovrebbero essere ancora più severi ed estesi in generale a tutto l'ambiente di Internet. Prima di commentare queste parole è giusto sottolineare la gravità dei problemi affrontati. Il bullismo è una cosa orribile ed è una parola che maschera spesso comportamenti semplicemente criminali. Non da meno è il problema della criminalità vera e propria e del terrorismo, che dietro la maschera dell'anonimato si muovono per le loro strategie. Sarebbe sbagliato e pericoloso minimizzare il problema. È la soluzione che lascia davvero perplessi. Anzitutto perché Facebook stesso è tutt'altro che un buon poliziotto del Web. Non sono pochi gli account creati su Facebook usando credenziali false e non è certo difficile creare un account senza fornire i propri dati personali. Noi stessi in redazione abbiamo almeno 2 account senza generalità esatte, perché siamo grandi fan della privacy. Ma il problema di Facebook non si ferma lì. Le notizie su reati legati alle attività sui social network sono quasi all'ordine del giorno. Delinquenti che rubano in casa delle persone tenendo d'occhio il loro stato, psicopatici che trovano sui social network donne da perseguitare, ecc. ecc. E non si parla solo di criminali ma anche di datori di lavoro che licenziano dipendenti dopo aver letto commenti "pepati" sulle loro bacheche. Insomma, Facebook può anche fare il paladino della lotta all'anonimato ma è poi il social network stesso a essere terreno fertile per attività che vanno dal problematico al pericolosissimo. C'è però un'altra questione sull'anonimato: chi dice che sia una cosa intrinsecamente negativa? C'è una serie di idee che la gente non ha alcuna intenzione di esprimere in un luogo pubblico nella vita reale. Per esempio, un tifoso che guarda una partita di calcio invitato da un amico nella curva della squadra avversaria difficilmente vorrà gridare al mondo cosa pensa del portiere che ha appena parato un rigore al suo attaccante preferito. Oppure è molto facile che una persona non voglia parlare delle sue idee politiche in un luogo in cui ci possono essere squilibrati pronti a usare la violenza come metodo di dialogo. Eppure i social network vorrebbero obbligarci a fare questo: ci esortano a mettere sulle loro reti i nostri pensieri più intimi e poi considerano l'anonimato una cosa sgradita. Anzi, sembra quasi che il "crimine" sia essere anonimi, non creare problemi ad altri sfruttando il fatto di sapere chi sono! Guardarsi in faccia, parlarsi e condividere idee sapendo con chi si ha a che fare è una bella cosa. Usare violenza testuale, verbale o fisica nei confronti degli altri sfruttando l'anonimato è una cosa orribile. Però l'anonimato deve rimanere una libera scelta e deve stare alla nostra coscienza collettiva e a forze dell'ordine e operatori di settore come Facebook fare in modo che la nostra libertà alla privacy e all'anonimato sia tutelata e che non venga viceversa sfruttata da altri per scopi illeciti o criminali.





NOTIZIE DAL MONDO HACKER

BATTERIE CRACKATE!

Si è appena conclusa la diciannovesima DefCon e già si spalancano le porte della Black Hat Conference, che riunisce i più importanti hacker del mondo. Tra i numerosi avvenimenti in programma, il più atteso è l'esibizione di Charlie Miller, che colpirà proprio il marchio a cui è tanto affezionato, vale a dire Apple.

SOTTO ACCUSA IL CHIP

Nella fattispecie, a finire nel mirino del tentativo di hacking saranno i chip di controllo delle batterie di alcuni Macbook, Macbook Pro e Macbook Air. Infatti Charlie Miller è riuscito a scoprire un punto debole proprio lì, un bug che riguarda le loro password di default. Nonostante la stranezza di questa porta d'accesso al sistema, il problema scoperto è piuttosto serio. Infatti, riuscendo a scoprirne i codici e attraverso la gestione del firmware, un eventuale malintenzionato potrebbe compiere qualsiasi tipo di azione nefasta, dal danneggiamento delle batterie stesse all'installazione di un malware non debellabile nemmeno con la reinstallazione del software. Questo malware sarebbe addirittura capace di surriscaldare le batterie e di farle esplodere!



BUCATE LE RETI GPRS

Karsten Nohl colpisce ancora! Il noto hacker con la passione per le comunicazioni via cellulare è riuscito a violare il sistema di cifratura delle reti GPRS. Forte dei successi avuti nel bucare le reti GSM, l'ex studente dell'Università della Virginia è riuscito a intercettare le comunicazioni GPRS nel raggio di 5 chilometri. A fare una pessima figura non sono state solo le società telefoniche tedesche, che userebbero algoritmi di cifratura facilmente aggirabili, ma soprattutto quelle italiane. Secondo gli studi effettuati da Nohl, le nostre telecomunicazioni sarebbero completamente prive di protezione!

I PREMI "MIO MINI PONY"

La quinta edizione del Pwnie Awards, in cui vengono premiati i peggiori Epic Fail dell'anno e gli hacker che li hanno provocati, si è appena conclusa con la classica pioggia di coloratissimi "Mio Mini Pony", il trofeo simbolo della manifestazione. Manco a dirlo, il primo premio è stato assegnato a Sony per la figuraccia fatta con la storia di Play Station Network (PSN) e il furto dei dati sensibili. Microsoft si è aggiudicata il "Mio Mini Pony" per il bug peggiore, riscontrato nel kernel win32k di Windows. Invece Juliano Rizzo e Thai Duong hanno vinto il premio per aver scoperto una vulnerabilità in ASP.NET Framework Padding Oracle.

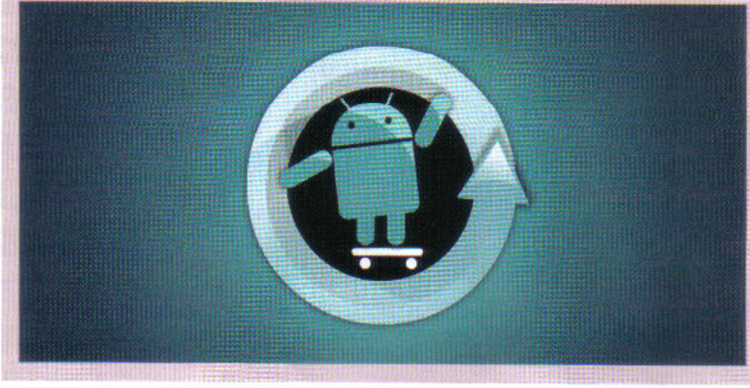


HTML5: BUCABILE?

In ben 61 pagine, l'European Network and Information Security Agency (ENISA) punta il dito contro i pericoli che creerebbero alcune caratteristiche del nuovo standard Web, l'HTML5. Nelle 13 specifiche analizzate si sono riscontrati addirittura 51 problemi di sicurezza! Uno di questi consentirebbe a un cybercriminale di farci cliccare sul pulsante sbagliato all'interno di una pagina Web, con evidenti conseguenze catastrofiche. Dell'intera relazione dovrà assolutamente tenere conto il World Wide Web Consortium (W3C), ente preposto a dare il via libera definitivo a questo nuovo standard e che non potrà ignorarne i rischi alla sicurezza che comporta.

SAMSUNG & CYANOGEN

Si chiama Steve Kondik ed è uno dei nomi di spicco nella comunità di sviluppatori di Android, ma è molto più famoso con il nick Cyanogen di CyanogenMod. Da poche settimane, il creatore del firmware per Android più famoso del mondo, è entrato a far parte della squadra della coreana Samsung, sebbene non si sia ancora capito esattamente quale ruolo coprirà. Comunque gli appassionati di CyanogenMod non hanno niente da temere, perché la squadra di sviluppo, composta da una quarantina di programmatori, resta in piedi e non perderà del tutto la preziosissima collaborazione di Kondik. Almeno così ha dichiarato Cyanogen nella sua pagina di Facebook in cui ha anche dato la notizia dell'assunzione.



LA FURIA DI ANTISEC

Si chiama campagna AntiSec ed è un'operazione di hacking su scala planetaria condotta dal gruppo cosiddetto hacktivist di Anonymous a cui si sono di recente uniti molti membri del disciolto LulzSec. Obiettivo principale di queste azioni cyberterroristiche (o cyberrivoluzionarie, dipende dal punto di vista) sono le istituzioni governative e certe aziende private che con esse collaborano.

10 GB DI BOTTINO

Il colpo inferto durante l'ultima azione è di quelli che si fanno ricordare e le sue vittime principali sono state ancora una volta le autorità di polizia. Il numero di siti attaccati con successo è impressionante: ben 76 sparsi per 11 stati americani. Comun denominatore è una società di marketing che ha sede in Arkansas, la Brooks-Jeffrey (www.bjmweb.com). Secondo quanto si legge nel comunicato ufficiale di Anonymous, in meno di 24 ore gli hacker sono riusciti a violare la sicurezza del server di Brooks-Jeffrey e a scaricare una quantità di dati pari a 10 GB. Il guaio è che si tratta di dati sensibili, informazioni riservate, indirizzi, numeri di codice della previdenza sociale americana e, soprattutto, numeri di carte di credito. Per sottolineare ancora una volta lo spirito che muove questi hacker, alcune carte di credito sono già state usate per effettuare donazioni ad associazioni per i diritti civili come American Civil Liberties Union (ACLU), Electronic Frontier Foundation e Bradley Manning Support Network.

SU SCALA MONDIALE

Gli attacchi non si sono però limitati al suolo statunitense. Anche Colombia, Ecuador e Siria hanno sentito il morso di AntiSec, che ha affondato le zanne nei loro siti degli Interni, della Giustizia e della Difesa. Insomma, il messaggio è chiaro: nessun Governo si senta al sicuro, perché quando Anonymous vorrà colpire lo farà in barba a qualsiasi sistema di difesa.





GUIDA

I SOFTWARE CONTENUTI NEL CD-ROM SONO SUDDIVISI IN 10 AREE TEMATICHE. ALCUNI DI ESSI SONO COLLEGATI AI TUTORIAL PUBBLICATI SULLA RIVISTA NELLE PAGINE CONTRASSEGNATE DAL LOGO "NEL CD".

HACKING

- Attack Tool Kit
- Avesoft Keylogger V2
- CL-NUI-Platform
- Firebug
- Firesheep
- FireMaster
- HttpWatch
- Take Ownership

INTERNET

- Filezilla Server
- Firefox 6
- FreshWebSuction
- Ip2Country
- Magento
- Tamper Data 11.0.1
- Tv Wave 037

PROGRAMMING

- Adobe Flash Player Deb.
- IronPyton
- MultiCode 1.17.0.2
- RAD Regex Designer
- SynWrite
- Virtual Box SDK
- Visual DuxDebugger
- Xelx

SECURITY

- Ccleaner 3.07.1457
- Crypt4Free
- Defensio
- Hallucinate
- HiJack Hunter
- RunScanner
- Secure Folder
- TrueCrypt

AL CD

UTILITY

- File Split
- Filezilla Client
- HJSplit
- Impulse 3.28.618
- Libre Office Portable
- Manage It!
- System Screensavers Tweaker
- YouTube Downloader

P2P

- BitTorrent
- BitTorrent Acceleration Tool
- Frostwire 4.21.3.
- PaSaMuf
- Portable µTorrent
- Skype 5.5.0.110
- Tribler

SYSTEM

- CheckDiskGUI
- D7 3.8.1
- Dataram Ramdisk
- Dropbox
- PartitionGuru 3.5.0
- Process Explorer
- Rsync
- Virtual Box
- Vistalizator

NETWORKING

- BitMeter OS 0.7.4 Beta
- iSpy
- KiTTY
- LAN Search Pro
- PHPMyAdmin
- Simple Internet Meter Lite

COPIARE

- Cdrtfe
- Copy N Size 5.0
- ExploreBurn
- ExtremeCopy 2.0.3
- FastCopy 32bit
- FastCopy 64bit
- FinalBurner Free
- FreeRIP
- HDClone Free Edition
- WinRichCopy

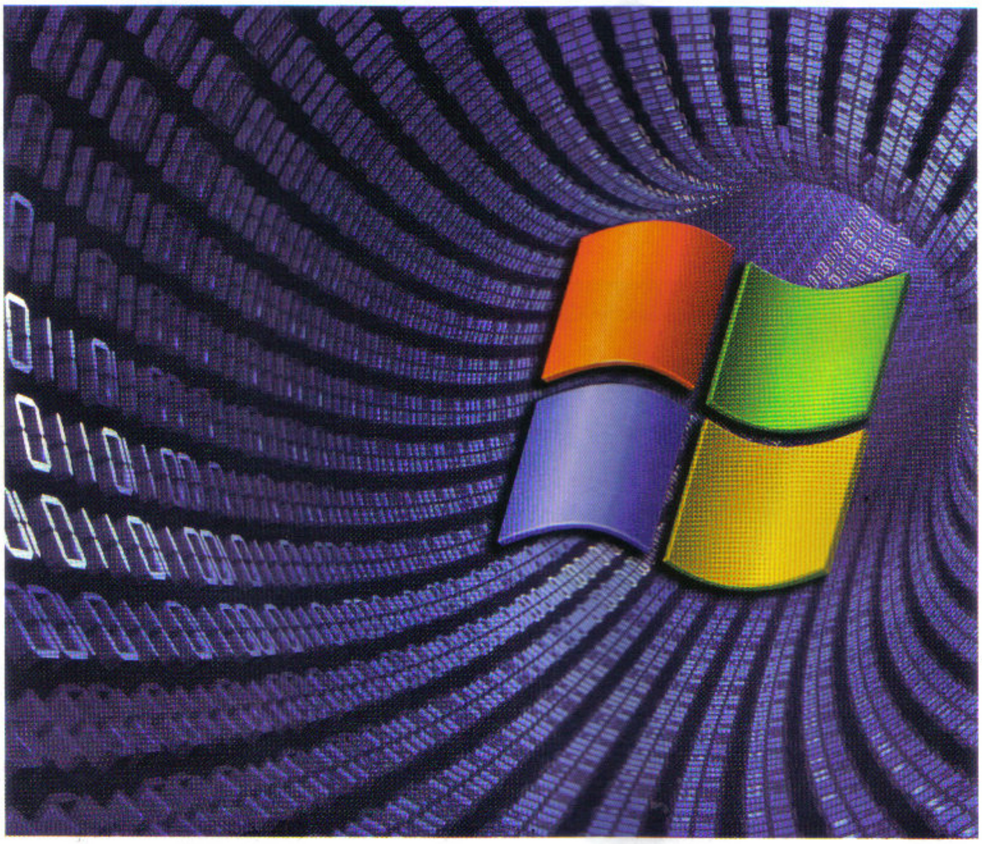
MULTIMEDIA

- Avidemux 2.5.4
- AWicons Lite
- BUFRDC 000387
- GMapCatcher
- Helium Audio Converter
- Kastor Free Audio Converter
- Screen2Avi
- VIP CD Ripper

7 SYSTEM

NEL CD

HACKERIAMO WINDOWS COL REGISTRO



PIEGHIAMO WINDOWS AL NOSTRO VOLERE METTENDO LE MANI SUL REGISTRO E ALTRE SUE PARTI GRAZIE A QUESTI 15 TRUCCHI

di Luca Facci
redazione@hakerjournal.it

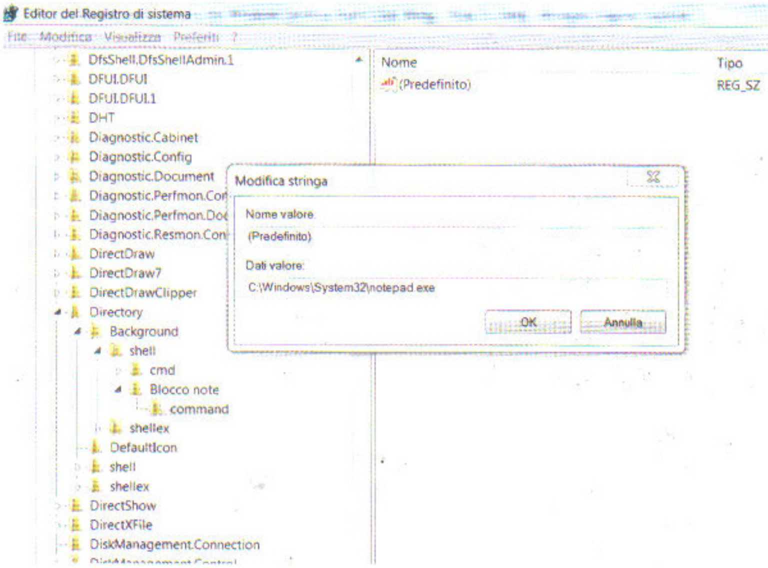
La semplificazione di un sistema operativo ha come effetto collaterale una forte limitazione alla sua personalizzazione. Ovviamente **Windows** non sfugge a questa regola. Quindi per fare in modo che sia lui a lavorare come vogliamo noi e non il contrario, dobbiamo mettere le mani alle sue parti più intime, come il **Registro**. Naturalmente, prima di fare qualsiasi modifica, creiamo un **punto di ripristino**, così non avremo guai.

1. IMPOSSESSIAMOCI DEI FILE DI SISTEMA

Chi usa **Vista** o **7** sa che impossessarsi dei file di sistema è una bella gatta da pelare. Invece noi lo faremo in modo semplice. Nella sezione **Hacking** del nostro CD, c'è il file **TakeOwnership.zip**. Decomprimiamolo, poi clicchiamo due volte sul file **InstallTakeOwnership.reg**. Quando appare la finestra intitolata **Editor del Registro di sistema**, clicchiamo sul pulsante **Sì** per confermare l'installazione, poi clicchiamo su **OK**. Ora ci basta cliccare con il pulsante destro su un file di sistema e selezionare **Take Ownership** nel menu contestuale e confermare con **Sì**. Per disinstallare questo **script**, clicchiamo due volte sul file **RemoveTakeOwnership.reg**.

2. RIAVVIAMO QUANDO VOGLIAMO

Dopo essersi aggiornato, **Windows** fa apparire una finestra di dialogo che ci costringe a riavviare il computer o ad attivare un promemoria. Purtroppo però questi



Per aggiungere un'applicazione qualsiasi al menu contestuale che appare cliccando con il pulsante destro sul Desktop, dobbiamo creare una chiave di Registro che contenga il percorso completo del file eseguibile.

promemoria finiscono e **Windows** ci avverte che si riavvierà comunque, ci piaccia o no. Per evitare questa scomodità, lanciamo l'**Editor del Registro di sistema** e apriamo la chiave *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows*. Se qui non c'è la chiave **WindowsUpdate**, dobbiamo crearla e, al suo interno, creiamo la chiave **AU**, con **Modifica/Nuovo/Chiave**. Apriamo **AU**, poi nel menu **Modifica** selezioniamo **Nuovo/Valore DWORD (32 bit)**. Chiamiamo la nuova chiave **NoAutoRebootWithLoggedOnUsers**, poi clicchiamoci sopra con il pulsante destro e selezioniamo **Modifica**. Nella finestra scriviamo **1** in **Dati valore**.

3. APPLICAZIONI NEL MENU CONTESTUALE

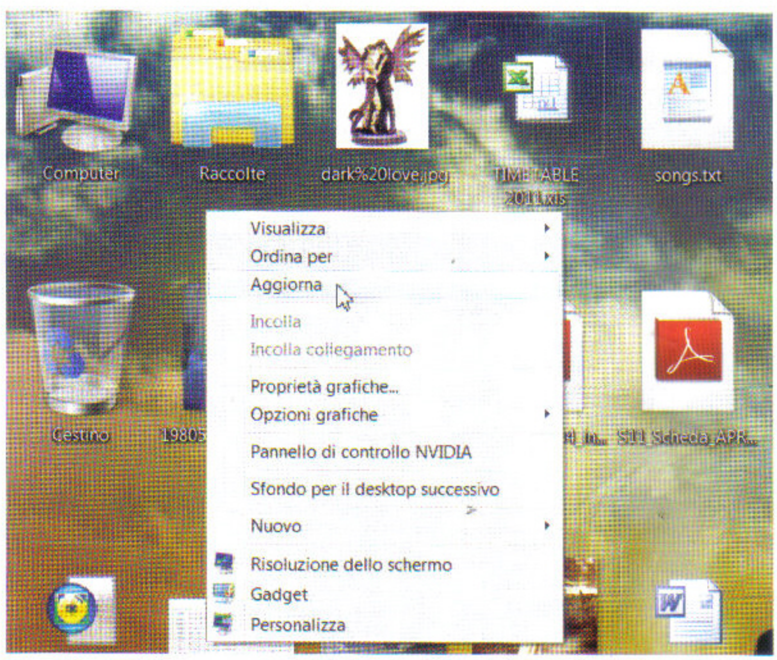
Se vogliamo aggiungere un'applicazione qualsiasi al **menu contestuale**, che si apre cliccando con il pulsante destro sul fondo di una finestra o del desktop, per averla immediatamente a disposizione, procediamo in questo modo. Nell'**Editor del Registro di sistema**, apriamo la chiave *HKEY_CLASSES_ROOT\Directory\Background\shell*. Creiamo una nuova chiave e chiamiamola con il nome del programma che vogliamo inserire nel **menu contestuale**, nel nostro esempio **Blocco note**. Poi creiamo la chiave di comando per lanciare l'applicazione. Clicchiamo con il pulsante destro sulla chiave appena creata e nel menu scegliamo **Nuovo/Chiave** e chiamiamo **command** quella nuova. Cerchiamo il percorso dell'applicazione da lanciare (nel nostro caso *C:\Windows\System32\notepad.exe*). Clicchiamo due volte su **(Predefinito)** della chiave **command** e, in **Dati valore**, incolliamo il percorso e clicchiamo su **OK**.

4. COLLEGAMENTI SENZA COLLEGAMENTO

Una delle cose più fastidiose e ridondanti che fa **Windows** è aggiungere la parola **collegamento** in fondo al nome delle icone dei collegamenti. Per togliergli questa brutta abitudine, avviamo l'**Editor del Registro di sistema** e apriamo la chiave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer*. A destra vediamo la chiave chiamata **link**. Clicchiamoci sopra due volte e, nella finestra che si apre, sostituiamo il valore **1** e la lettera che segue con **00** (doppio zero). Poi confermiamo con **OK**. Purtroppo questa modifica non influenza i collegamenti già esistenti, ma solo quelli che creeremo da ora in poi.

5. LE RACCOLTE SUL DESKTOP

Avere la cartella **Raccolte** funzionante sul nostro **Desktop**, non solo un semplice collegamento, è un gioco da ragazzi. Ovviamente dovremo agire tramite l'**Editor del Registro di sistema**, quindi lanciamolo e apriamo la chiave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel*. Poi, nel menu **Modifica**, clicchiamo su **Nuovo/Valore DWORD (32 bit)** e chiamiamolo **{031E4825-7B94-4dc3-B131-E946B44C8DD5}** lasciandolo a valore **0**. Ora chiudiamo l'**Editor del Registro di sistema** e trasferiamoci sul **Desktop**. Clicchiamo con il pulsante destro su una zona vuota e, nel menu contestuale, scegliamo **Aggiorna**. Così vedremo comparire la cartella **Raccolte**.

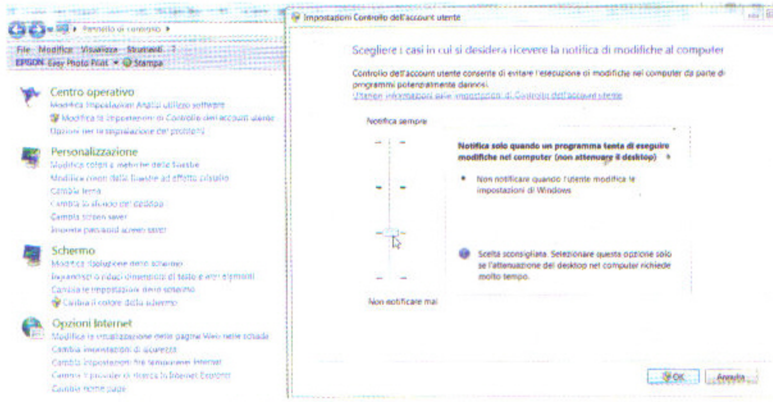


Grazie a una veloce modifica alla chiave del Registro HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel, possiamo visualizzare sul Desktop la cartella Raccolte, così non dovremo più usare il menu Start.

6. UN RIPRISTINO PARZIALE

Non sempre è utile ripristinare tutto il sistema operativo da un **punto di ripristino** precedente, perché così perdiamo certe modifiche che desideriamo mantenere. Per fortuna, **Windows 7** ci permette di farne uno parziale.

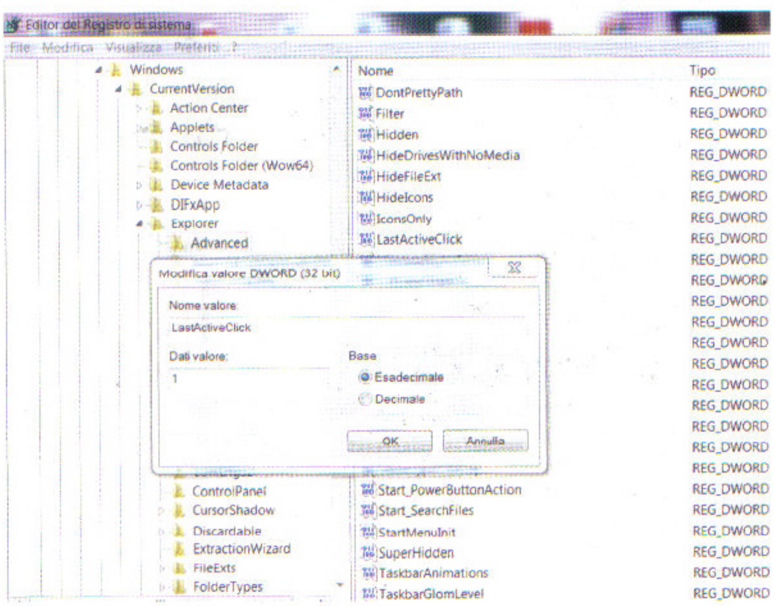
Per prima cosa apriamo il **Pannello di controllo** e, nel campo di ricerca, scriviamo **modifica**. Sotto la voce **Centro operativo**, troveremo **Modifica le impostazioni di Controllo dell'account utente**. Clicchiamoci sopra, poi abbassiamo completamente il cursore che vediamo nella finestra. Riavviamo il computer. Ora apriamo la cartella **config** che si trova in *C:\Windows\System32*. Clicchiamo con il pulsante destro in una zona vuota della cartella e nel **menu contestuale** scegliamo **Proprietà**, poi apriamo la scheda **Versioni precedenti**. Scegliamo la cartella **config** con la data del ripristino che vogliamo e clicchiamoci sopra due volte. A questo punto, selezioniamo i file da ripristinare e copiamoli dentro una cartella qualsiasi. Ora apriamo l'**Editor del Registro di sistema** e selezioniamo la chiave *HKEY_LOCAL_MACHINE* oppure *HKEY_USERS*. Nel menu **File**, clicchiamo su **Carica hive**, dopodiché clicchiamo sui file copiati. Apparirà una finestra in cui dovremo inserire il **Nome chiave**. Per esempio scriviamo **Prova** e clicchiamo su **OK**.



Per poter fare un ripristino parziale del nostro sistema operativo, dobbiamo prima di tutto modificare le impostazioni di controllo del nostro account utente, disabilitando completamente le notifiche, tramite il cursore che vediamo sulla sinistra della finestra.

7. L'ULTIMA FINESTRA ATTIVA

Chi usa **Windows 7** avrà sicuramente imparato ad apprezzare le caratteristiche di **Aero Peek** che ci permette di visualizzare le anteprime delle finestre aperte, direttamente dalla **Barra delle applicazioni**, per poter scegliere quella che vogliamo. Tuttavia possiamo ulteriormente migliorare questo strumento perché ci mostri sempre l'ultima finestra aperta, senza dover ricorrere al pulsante **Ctrl**. Apriamo come al solito l'**Editor del Registro di sistema** e selezioniamo la chiave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced*. Nel menu **Modifica**, clicchiamo su **Nuovo/Valore DWORD (32 bit)** e chiamiamo questa chiave **LastActiveClick**. Clicchiamoci sopra due volte e, nel campo **Dati valore**, scriviamo **1** al posto di **0**. Clicchiamo su **OK** e riavviamo.



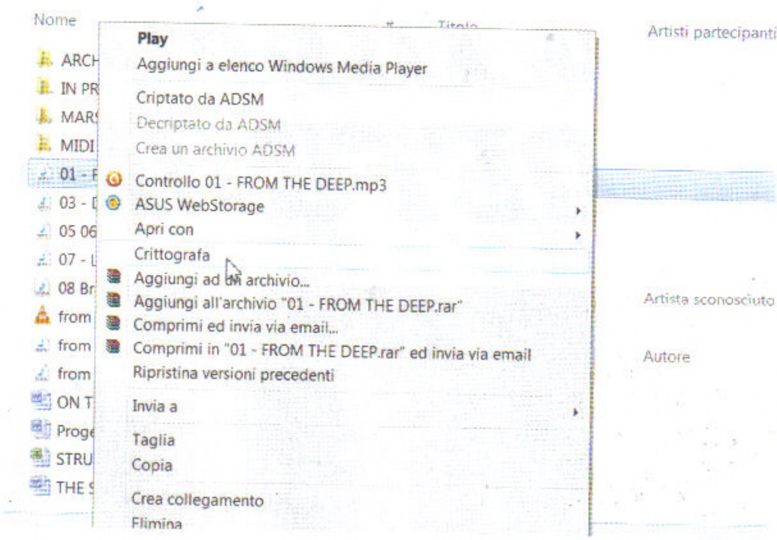
Con questa semplicissima modifica al Registro di sistema riusciremo a rendere più efficiente lo strumento Aero Peek di Windows 7 e avremo sempre a portata di clic l'ultima finestra aperta, senza doverla andare a cercare tra le tante che abbiamo aperto.

8. UNA VERA PULIZIA

Sembra assurdo, eppure la funzione **Pulizia disco** di **Windows** in realtà non pulisce i file temporanei, a meno che non siano più vecchi di 7 giorni. Naturalmente possiamo fare in modo che le cose vadano diversamente e fare davvero pulizia nel nostro disco fisso. Lanciamo l'**Editor del Registro di sistema** e selezioniamo quindi la chiave *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Temporary Files*. A destra, clicchiamo due volte su **LastAccess** e, nel campo **Dati valore**, scriviamo il numero di giorni che vogliamo, per esempio **1**, poi confermiamo con **OK**.

9. MODIFICHIAMO IL MENU START

Se non amiamo molto il nuovo menu **Start** di **Windows 7**, possiamo modificarlo perché assomigli un po' di più a quello di **XP**. Nell'**Editor del Registro di sistema** selezioniamo *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders*. Clicchiamo due volte su **Favorites** e modifichiamo **Dati valore** con **C:\ProgramData\Microsoft\Windows\Start Menu\Programs**. Confermiamo con **OK**. Apriamo la chiave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*, clicchiamo due volte su **Favorites** e ripe-



Per inserire nel menu contestuale di Windows Vista o 7 il comando Crittografa, basta una semplicissima modifica alla chiave del Registro di sistema HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced.

tiamo l'operazione precedente. Chiudiamo il **Registro di sistema**, clicchiamo con il pulsante destro sul menu **Start** e poi su **Proprietà**. Nella finestra clicchiamo su **Personalizza** e nell'elenco troviamo la voce **Menu Preferiti**. Selezioniamola e clicchiamo su **OK**, poi riavviamo.

10. CIFRIAMO CON WINDOWS

Con questa piccola modifica al **Registro di sistema**, potremo avere lo strumento **Crittografa** nel menu contestuale di **Windows Vista** e **7**. Lanciamo l'**Editor**, poi apriamo la chiave *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced*. Nel menu **Modifica**, selezioniamo **Nuovo/Valore DWORD (32 bit)** e chiamiamolo **EncryptionContextMenu**. Clicchiamoci sopra due volte e diamogli valore **1**.

11. PERSONALIZZARE GLI SCREEN SAVER

Windows Vista e **7** non ci fanno personalizzare come vorremo gli **Screen saver** disponibili. Decomprimiamo il file **System_Screensavers_Tweaker.zip** che troviamo nel nostro CD, poi lanciamo il file **nt6srccfg.exe**. Selezioniamo uno dei 4 **Screen saver** disponibili e modifichiamolo a piacere, usando le opzioni e i cursori che appaiono in ciascuna scheda.

12. SCEGLIAMO IL PROGRAMMA

Per eliminare la fastidiosa finestra che ci chiede se vogliamo cercare sul **Web** il programma per aprire un file o sceglierlo personalmente, apriamo la chiave del **Registro di sistema** *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer*. Creiamo un nuovo **valore DWORD 32 bit** e chiamiamolo **NoInternetOpenWith**, poi diamogli valore **1**.

13. DEFRAG CON UN CLIC

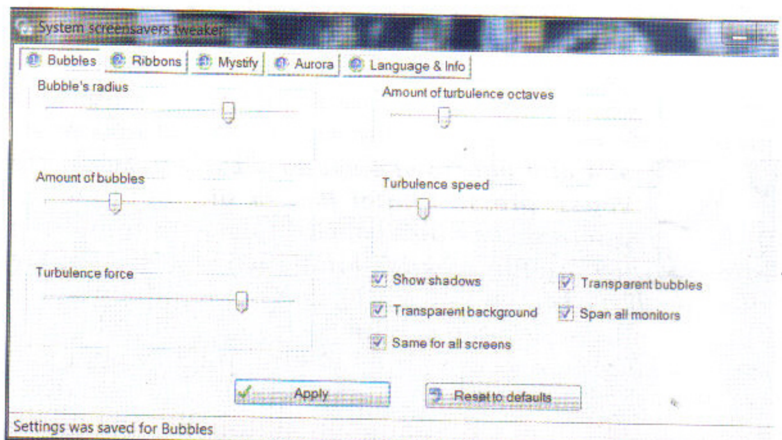
Per avere il comando **Deframmenta** nel menu contestuale del disco fisso, nella chiave del **Registro di sistema** *HKEY_CLASSES_ROOT\Drive\shell* creiamo la chiave **runas**. Clicchiamo quindi due volte su **(Predefinito)** e inseriamo il valore **Deframmenta**. Poi in **runas** creiamo la chiave **command** e in **(Predefinito)** inseriamo **defrag %1 -v**.

14. PANNELLO DI CONTROLLO PRATICO

Per aggiungere l'icona del **Pannello di controllo** alla cartella **Computer**, apriamo la chiave del **Registro di sistema** *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace* e aggiungiamo la chiave **{21EC2020-3AEA-1069-A2DD-08002B30309D}**.

15. L'ICONA DI INTERNET EXPLORER

Se rivogliamo la vecchia icona di **Internet Explorer** anche in **Windows 7**, nell'**Editor del Registro di sistema** selezioniamo la chiave *HKEY_CLASSES_ROOT\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}* con il pulsante destro del mouse e clicchiamo su **Esporta**. Chiamiamo il file **ie-guid.reg** e salviamolo. Apriamolo con il **Blocco note** e, in **Modifica**, selezioniamo **Sostituisci**. In **Trova** scriviamo **{871C5380-42A0-1069-A2EA-08002B30309D}** e in **Sostituisci con** scriviamo **{871C5380-42A0-1069-A2EA-08002B30301D}**, poi clicchiamo su **Sostituisci tutto** e salviamo il file. Clicchiamoci sopra due volte per ripristinarlo. Ora nel **Registro di sistema** apriamo la chiave *HKEY_CLASSES_ROOT\CLSID\{871C5380-42A0-1069-A2EA-08002B30301D}\Shellex\ContextMenuHandlers\ieframe*, clicchiamo due volte su **(Predefinito)** e inseriamo il valore **{871C5380-42A0-1069-A2EA-08002B30309D}**. Visualizziamo il **Desktop**, premiamo **F5** e riavremo la vecchia icona e il suo **menu contestuale**.



Per personalizzare i nostri Screen saver, usiamo il semplicissimo programma System screensavers tweaker che troviamo nella sezione Utility del CD di Hackers Magazine.

ANDROID TREMA ALLA DEFCON



FALLE IN ANDROID, BAMBINI TERRIBILI CHE AGGIRANO LE PROTEZIONI DEI VIDEOGIOCHI E MOLTO ALTRO ANCORA ALLA DEFCON 2011 DI LAS VEGAS: VEDIAMO COME È ANDATA...

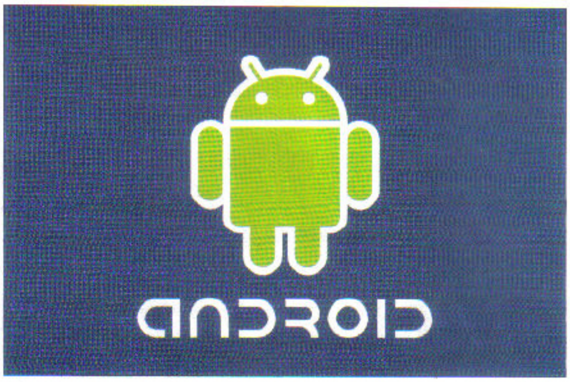
di Domenico Castolo
redazione@hackerjournal.it

Dal 4 al 7 agosto si è svolta a Las Vegas, presso l'Hotel Rio, la diciannovesima DefCon, cioè la più importante manifestazione mondiale degli hacker. Qui, i vari gruppi o i "lupi solitari" si riuniscono per confrontarsi e per svelare le vulnerabilità scoperte nel corso dell'anno. Ma anche per sfidarsi in gare informatiche all'ultimo hacking.

LA FALLA DI ANDROID

Anche quest'anno, il programma è stato piuttosto succoso e ha riservato la sua buona dose di sorprese, che talvolta sembrano dei veri e propri fulmini a ciel sereno nel mondo già turbolento dell'informatica. Sicuramente la notizia che ha fatto sobbalzare più di una persona sulla sedia è stata la scoperta da parte di due ricercatori (**Sean Schulte** e **Nicholas Percoco**) di una falla in **Android**. Falla che, se opportunamente sfruttata, metterebbe in pericolo i vari smartphone e tablet funzionanti con il sistema operativo di **Google**. Si tratta di un difetto di progettazione, un'ingenuità che potrebbe però avere conseguenze nefaste. In sostanza, proprio la capacità di **Android** di permettere a un'applicazione di comunicare con l'utente mentre ce n'è un'altra in primo piano, permetterebbe la creazione di finte schermate allo scopo di ingannare l'utente e spingerlo a inserire dati personali con una classica operazione di **phishing**. Nella

dimostrazione dei due ricercatori, del codice maligno all'interno dell'applicazione di **Facebook** permette a un hacker di far saltare in primo piano un'app che, come nel phishing tradizionale, mostra una schermata di login identica a quella dell'app genuina, senza che il sistema operativo dia alcun allarme poiché il codice sfrutta una funzione perfettamente legittima. L'unico modo di accorgersi della cosa è un brevissimo "flash", appena percettibile, che scatta quando la schermata dell'app pirata viene messa in primo piano. Google minimizza ma la verità è che il mercato di Android potrebbe subire un colpo non da poco se si diffondessero applicazioni così pericolose.



Il sistema operativo per dispositivi mobili, marcato Google, è stato uno dei protagonisti della DefCon 2011, in cui due ricercatori ne hanno svelato una pericolosa vulnerabilità.

PICCOLI HACKER CRESCONO

DefCon ha una sezione riservata agli hacker più giovani e anche qui se ne vedono delle belle, considerata l'età dei partecipanti. È il caso, per esempio, di una ragazzina di appena 10 anni che, stufa dei tempi di attesa che le venivano imposti da un videogioco per smartphone, ha pensato di porvi personalmente rimedio. In pratica ha staccato il collegamento **WiFi** e ha mandato avanti l'orologio del proprio dispositivo mobile. Così le piantagioni di questo gioco stile **Farmville** sono arrivate istantaneamente a maturazione. Tuttavia **CyFi**, così si fa chiamare questa astuta hacker in erba, non ha voluto rivelare il nome del gioco hackerato. Questo ha spinto gli organizzatori della **DefCon** a lanciare un concorso. Il primo che scoprirà il nome della "vittima" di **CyFi** vincerà 100 dollari. Comunque la sezione giovanile della **DefCon** non esiste solo per sfoggiare le imprese di ragazzini come **CyFi**, ma ha anche degli scopi più edificanti. Infatti, da quest'anno, si sono svolti dei veri e propri corsi, non solo per dare ai giovani dagli 8 ai 16 anni le conoscenze per svolgere operazioni efficaci di hacking, ma soprattutto per educarli all'etica dell'hacking stesso, le cui azioni sono principalmente preventive e mai criminali. Per esempio, gli appartenenti alla sezione **DefCon Kids** hanno potuto parlare con agenti delle varie agenzie di sicurezza americane a proposito di operazioni di investigazione informatica, spionaggio, eccetera.



Questa giovanissima "hacker" di appena 10 anni è riuscita a scoprire una falla all'interno di un gioco sociale tipo Farmville, che le ha permesso di saltare i lunghi tempi di attesa tra un'operazione e l'altra.

ANON PLUS

Un altro avvenimento che non poteva passare sotto silenzio è stata la presentazione del nuovo **social network** creato dall'anarchica **Anonymous** (*http://anonplus.bombshellz.net*), associazione che si batte contro la censura governativa in generale, schierandosi dalla parte della libera circolazione delle informazioni. Il nome nasce molto probabilmente come risposta a **Google+**, che li ha cacciati di recente. Quindi la kermesse mondiale degli hacker è diventata un naturale trampolino di lancio per **Anon Plus** e proprio per l'occasione è stato presentato il "manifesto" della neonata rete sociale e alcune iniziative che vedranno presto la luce. Tra queste, viene preannunciato il varo di un ambiente educativo **OpenSource** in pieno stile cyberanarchico in cui la pace dovrebbe "venire mantenuta attraverso la comprensione tra i membri stessi e non con la forza o le minacce". Ora che **DefCon 2011** ha chiuso i battenti, vedremo quali ricadute pratiche si avranno nel mondo informatico, fisso e mobile, in seguito alle scoperte fatte dai vari partecipanti. Sicuramente si cercherà di tappare la falla di **Android**, come di impedire a qualche giocatore di coltivare asparagi troppo velocemente. In ogni caso, tutto quanto successo non cadrà nel dimenticatoio, in attesa che il 2012 ci porti una nuova **DefCon** e nuove magagne smascherate.



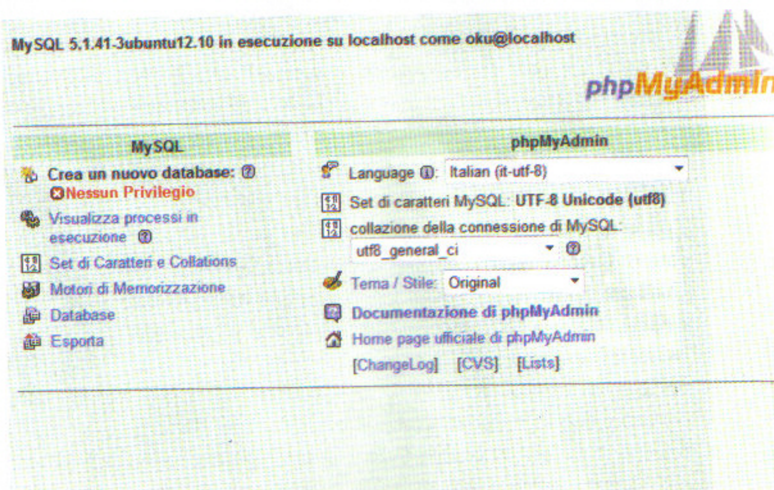
TOH, CHI SI RIVEDE... MITNICK!

A DefCon 2011 ha partecipato, autografando le copie del suo libro *The Art of deception*, anche **Kevin Mitnick**, il "re degli hacker", che iniziò le sue attività nel 1981 ad appena 17 anni, riuscendo a reindirizzare a piacere le chiamate di un server telefonico. Due anni dopo compì la sua impresa più importante, penetrando in un computer del Pentagono. Divenuto un bersaglio dell'FBI, fu arrestato nel 1995, dopo essere riuscito a evitare più volte la cattura. Condannato a scontare cinque anni di carcere, fu liberato nel 2000. Attualmente è proprietario di una società che si occupa di sicurezza informatica, la **Mitnick Security Consulting LLC**.

HACKING

LO SCRIPT DEL MESE
PHPMYADMIN
COMODITÀ SENZA PARI

PER COLORO CHE SMANETTANO CON MYSQL ECCO UN PANNELLO ELEGANTE E FACILE DA USARE PER LA GESTIONE DEI NOSTRI DATABASE. VEDIAMO COME OTTENERLO E QUALI SONO LE SUE PRINCIPALI FUNZIONI



di Domenico Castolo
redazione@hackerjournal.it

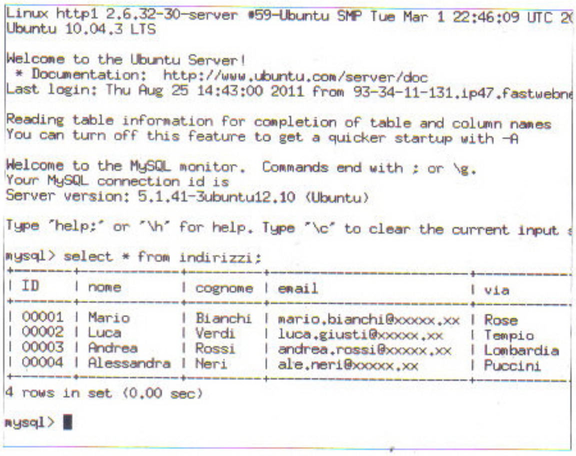
La gestione di un database MySQL può essere complicata, ed è bene avere gli strumenti giusti per non avere problemi. Creare tabelle, inserire record e visualizzare risultati di una ricerca sono tutte cose che possiamo fare da un terminale collegati al nostro database. Ma non è certo la cosa più pratica che ci sia. Per questo motivo troviamo su Internet una serie di pannelli di facile configurazione che meglio si adattano alle nostre necessità. Il più famoso e forse anche il più completo è phpMyAdmin che troviamo nel CD allegato a questo numero oppure all'indirizzo *www.phpmyadmin.net*. Per funzionare richiede un server Web come quello di Apache e il supporto del linguaggio PHP mentre con un qualsiasi browser potremo visualizzarne le pagine.

COME SI INSTALLA?

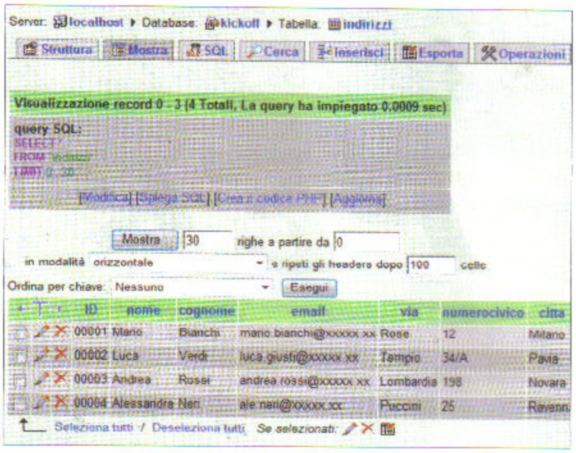
Il pannello di amministrazione phpMyAdmin viene fornito all'interno di un archivio che dobbiamo decomprimere in una cartella. Partendo dal presupposto che il server web e MySQL siano già installati e attivi sul nostro sito, per poter usare il pannello dobbiamo semplicemente caricare nel nostro sito o in locale la cartella decompressa. Modifichiamo il file di configurazione config.inc.php inserendo dove richiesto i giusti valori come nome utente e password (necessaria solo se come metodo di autenticazione lasciamo 'config'). Basta ora andare all'indirizzo *www.ilmiosito.it/cartelladelpannello/index.php* per vedere la schermata principale del nostro amministratore di database.

TUTTO CON UN CLIC

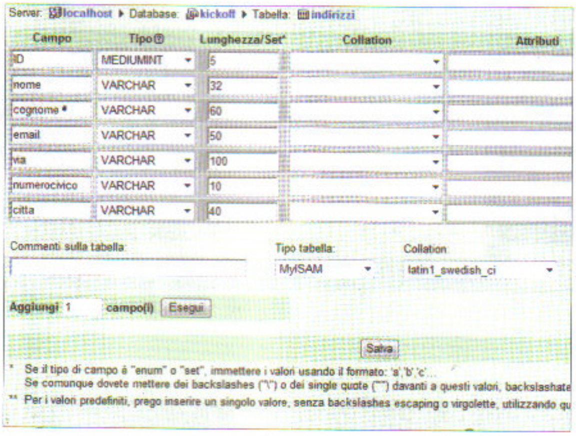
La comodità di questo pannello è che con un semplice clic possiamo fare molte cose che ci evitano di scrivere lunghe query con il terminale. Per esempio, dopo che abbiamo cliccato sul nome di una tabella per vederne la struttura, clicchiamo su **Mostra** per visualizzarne i record o su **Svuota** per eliminare tutto il suo contenuto. Altrimenti clicchiamo su **Elimina** per eliminare la tabella stessa. Clicchiamo invece sul nome di uno dei campi della tabella per ordinare i dati secondo il campo scelto, l'ordinamento sarà ascendente. Clicchiamo nuovamente sul nome del campo per l'ordinamento discendente. Se invece siamo nostalgici del terminale, phpMyAdmin ci offre uno strumento per scrivere comunque le query e vederne poi i risultati. Ogni query viene poi riproposta dopo l'esecuzione e può essere modificata semplicemente cliccando su **Modifica**. Se invece clicchiamo su **Spiega SQL** potremo avere alcune informazioni sul risultato della query come i nomi delle tabelle interessate e il numero di righe visualizzate. Ci sono poi una serie di funzioni, che troviamo cliccando su **Operazioni**, che ci permettono sempre con un clic, di rinominare, duplicare o spostare una tabella. Quando duplichiamo una tabella possiamo scegliere se duplicare solo la struttura oppure se mettere anche i dati per avere così una copia esatta della tabella d'origine. Ci sono inoltre una serie di funzioni di importazione ed esportazione dei dati che forse saranno pane per gli utenti più esigenti ma che sono comunque facilissime da eseguire, sempre con il solito clic.



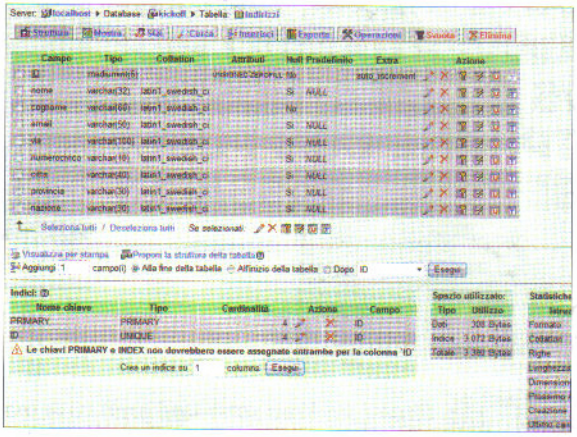
Ecco il risultato di una semplice query con il terminale. Abbiamo voluto vedere il contenuto di una tabella. In questo caso la visualizzazione dei risultati è anche abbastanza chiara ma quando ci troviamo con molti più risultati lo schermo diventa quasi illeggibile.



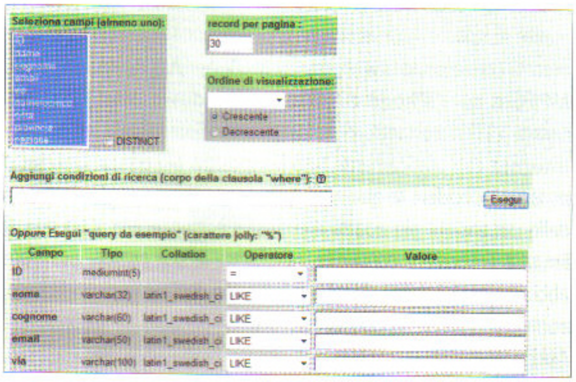
Ecco invece come viene visualizzato lo stesso contenuto della tabella con il pannello phpMyAdmin. L'interfaccia grafica è decisamente più chiara e con un clic modifichiamo, ordiniamo, cancelliamo e molto altro. Inoltre abbiamo molte informazioni in più sulla query appena eseguita.



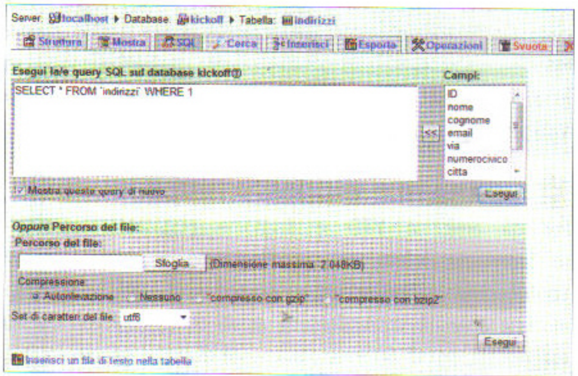
Da un'unica schermata possiamo creare una tabella e tutti i suoi campi. Inseriamo il nome e il tipo di ogni campo specificandone la lunghezza e, se vogliamo, il valore predefinito che quel campo deve assumere automaticamente dopo ogni inserimento di un record.



La visualizzazione della struttura di una tabella ci permette di ottenere velocemente tutti i dati dei suoi campi. Clicchiamo sull'icona che rappresenta una matita per modificare un campo. Nella parte bassa vediamo anche una serie di statistiche che indicano lo spazio utilizzato e il numero di righe della tabella.



*Ricercare i dati all'interno di una tabella è molto semplice: basta specificare il valore che ci interessa di uno o più campi e cliccare su **Esegui** per vedere quali record soddisfano le nostre condizioni. Possiamo anche stabilire quanti risultati vedere in una singola pagina e l'ordine di visualizzazione.*



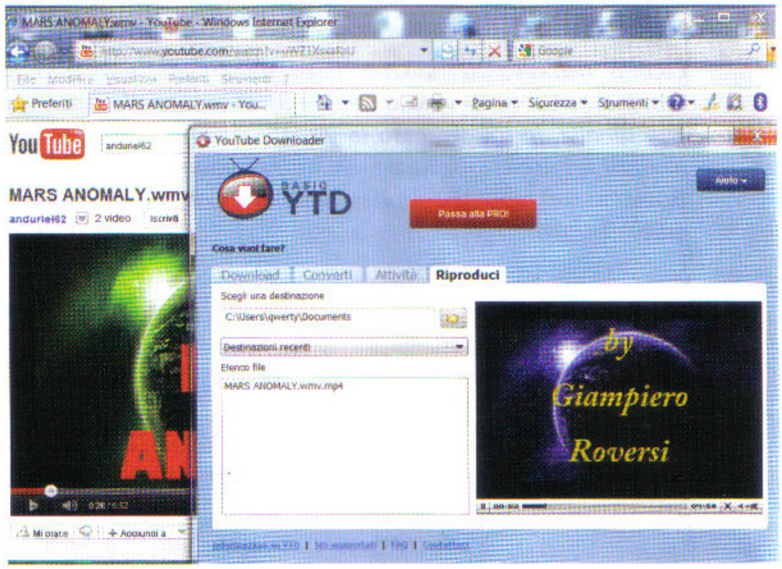
*Questo riquadro è dedicato a tutti coloro che vogliono scrivere le query senza invece cliccare sui collegamenti che ci sono nel pannello. Clicchiamo su **Esegui** per avviare il comando che scriviamo. Da questa finestra possiamo anche importare i dati nella tabella da un file di testo.*

MULTIMEDIA

NEL CD

TUTTI I VIDEO PER NOI!

SCARICHIAMO TUTTI I FILMATI CHE VOGLIAMO DA YOUTUBE, FACEBOOK, YAHOO VIDEO E GOOGLE VIDEO, QUINDI CONVERTIAMOLI PER WINDOWS O PER IL NOSTRO SMARTPHONE CON POCHI E SEMPLICI PASSAGGI

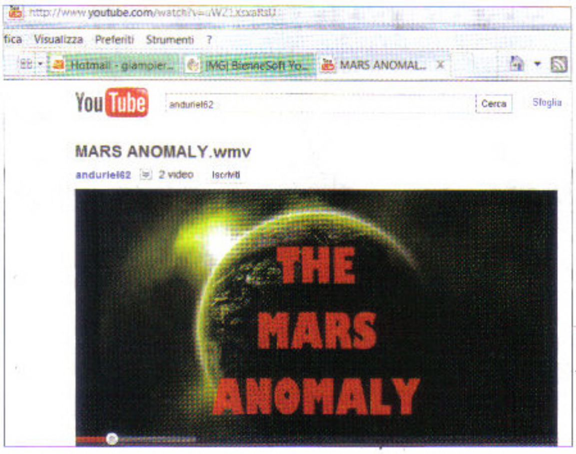


di redazione@hackerjournal.it

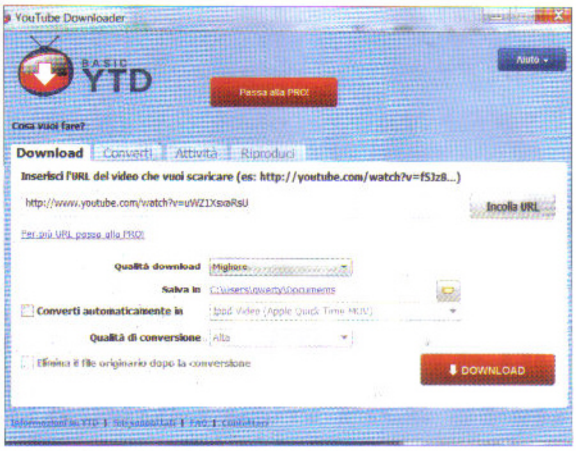
I filmati sul Web sono una gran cosa ma spesso ci piacerebbe averli sul nostro disco fisso per rivederli offline. Quando ci colleghiamo ai nostri siti di filmati preferiti, come **YouTube**, **Yahoo Video** e **Google Video**, non c'è alcun modo per poter scaricare i video che troviamo e, per poterli rivedere, siamo costretti a salvare l'indirizzo **Internet** nei nostri **Preferiti** oppure a usare specifici strumenti per i singoli siti Web per scaricare in qualche formato il filmato. Quello di cui abbiamo bisogno è uno strumento pratico per poter salvare i filmati che ci piacciono di più da qualsiasi servizio Web e nel formato che preferiamo noi in modo semplice e rapido. Quello di cui abbiamo bisogno si chiama **YouTube Downloader.**

VERSATILE E COMPATIBILE

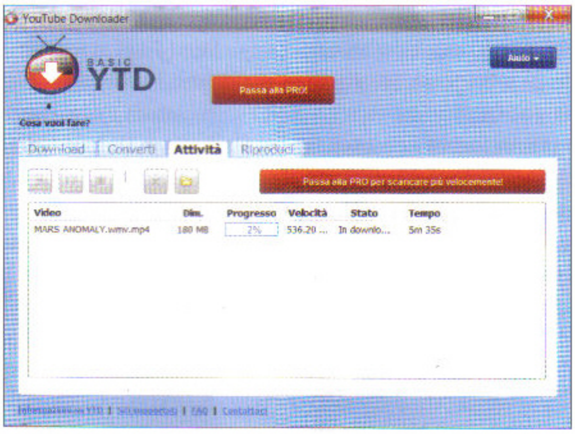
Per gli amici è **YTD** e il nome può essere alquanto fuorviante. Infatti, se ci colleghiamo all'indirizzo *www.youtubedownloadersite.com/supported_sites.html*, scopriremo una quantità impressionante di siti compatibili con questo programma: più di 60 e assolutamente di tutti i generi! Inoltre, **YTD** ha un ulteriore vantaggio che non risulta mai spiacevole: dalla versione **3.3** è anche completamente in italiano. L'unico vero neo di questo programma è che ne esistono due versioni, quella base e la **Pro**, che costa 19,90 dollari. Per questa cifra, avremo alcuni vantaggi in più. Per esempio potremo scaricare più filmati contemporaneamente e a una velocità fino a 4 volte superiore. Inoltre potremo convertire direttamente i video mentre li stiamo scaricando. Dalle prove che abbiamo fatto con il programma ci riesce abbastanza difficile consigliare l'acquisto della versione **Pro**. A parte la possibilità di scaricare più video contemporaneamente, non vediamo altri vantaggi concreti. Infatti la possibilità di scaricare più velocemente è tutta da dimostrare, visto che il programma ha sfruttato molto bene la banda a disposizione anche nella sua versione base! A parte ciò, **YTD** il suo dovere lo fa piuttosto bene. Come vediamo nella guida qui accanto, tutte le procedure di scaricamento, conversione e visualizzazione dei filmati sono estremamente semplici e intutive. A nostra disposizione abbiamo ben 7 formati di conversione diversi, tra cui **MOV** per **Apple Quick Time**, **MPEG-4** per l'**iPhone** e **WMV** per **Windows Media Player**. Quindi **YTD** ci permette di rendere compatibili i video scaricati da **Internet** con praticamente tutti i dispositivi più diffusi. Oltretutto possiamo decidere la qualità del file convertito, in modo da averlo delle dimensioni più adatte alle nostre esigenze. Ma **YTD** non si limita a scaricare e convertire, perché tra le sue opzioni avanzate abbiamo la possibilità di agire sul volume dell'audio di un filmato, aumentandolo se troppo basso, o diminuendolo se troppo alto. Anche l'opzione di ritaglio può essere molto utile. Per esempio, se di un filmato ci interessa una parte, possiamo convertire solo quella, indicandone il punto di inizio e di fine in ore/minuti/secondi. Naturalmente con **YTD** possiamo convertire qualsiasi tipo di file video compatibile, non solo quelli dei siti in elenco. **YTD** non offre funzioni rivoluzionarie: possiamo scaricare filmati da YouTube da parecchio tempo. Quello che offre però è compatibilità estrema, tantissimi formati e pratiche opzioni: imperdibile.



Avviamo il nostro programma di navigazione ***Internet*** *e, per esempio, colleghiamoci a* ***YouTube****. Cerchiamo il filmato che ci interessa scaricare e colleghiamoci con la sua pagina. A questo punto non dobbiamo far altro che selezionarne l'indirizzo e copiarlo.*



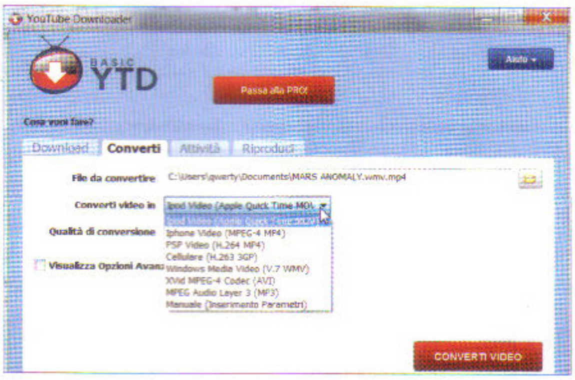
Ora avviamo ***YouTube Downloader****. Nella scheda* ***Download****, incolliamo l'indirizzo appena copiato, usando il pulsante* ***Incolla URL****, oppure clicchiamo sul campo in alto e premiamo* ***Ctrl+V****. Poi, nel menu a tendina* ***Qualità download****, selezioniamo una delle opzioni presenti.*



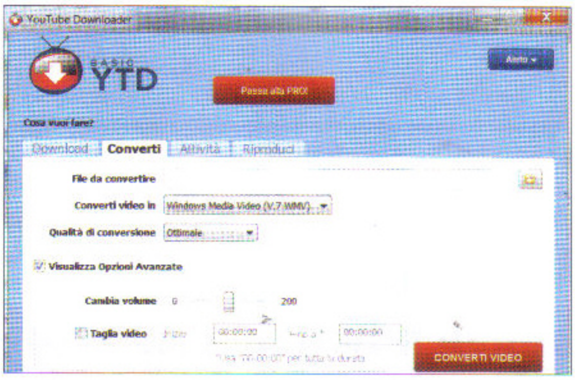
A questo punto possiamo decidere di scaricare il filmato, oppure convertirlo immediatamente (solo con la versione ***Pro****). Nel primo caso, non dobbiamo far altro che cliccare sul pulsante* ***Download****. Verrà automaticamente visualizzata la scheda* ***Attività*** *in cui potremo seguire il progresso dell'operazione.*



Terminato il download, sempre nella scheda ***Attività****, clicchiamo sull'icona a forma di cartella per visualizzare la posizione del file (normalmente la cartella* ***Documenti****). Per vederlo, apriamo la scheda* ***Riproduci****, inseriamone il percorso nel primo campo, poi selezioniamolo in* ***Elenco file****.*



Per convertire il file scaricato, apriamo la scheda ***Converti*** *e, nel campo* ***File da convertire****, inseriamo il percorso. Nel menu* ***Converti video in****, scegliamo il tipo di file in cui vogliamo trasformare il filmato quindi, in* ***Qualità di conversione****, scegliamo quella che preferiamo. Poi clicchiamo su* ***Converti Video****.*



Se durante la conversione vogliamo modificarne il volume, sempre nella scheda ***Converti****, selezioniamo* ***Visualizza Opzioni Avanzate*** *quindi usiamo il cursore* ***Cambia volume****. Per convertirne solo una parte, selezioniamo* ***Taglia video*** *e indichiamone l'inizio e la fine.*

NASCONDERE I NOSTRI FILE

GETTIAMO FUMO NEGLI OCCHI A CHI VUOLE CURIOSARE TRA I NOSTRI FILE RISERVATI

di Raffaele Malazzi
redazione@hackerjournal.it

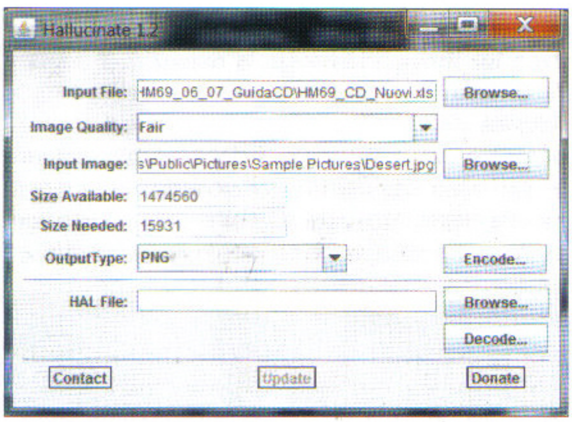
I nostri dati personali sono costantemente oggetto di desiderio da parte di un sacco di malintenzionati su Internet, mentre i nostri file possono suscitare inopportune curiosità da parte di qualche collega o qualche famigliare ficcanaso. In poche parole non possiamo mai stare un attimo tranquilli e dobbiamo continuamente guardarci le spalle per evitare di subire furti informatici.

SOTTO MENTITE SPOGLIE

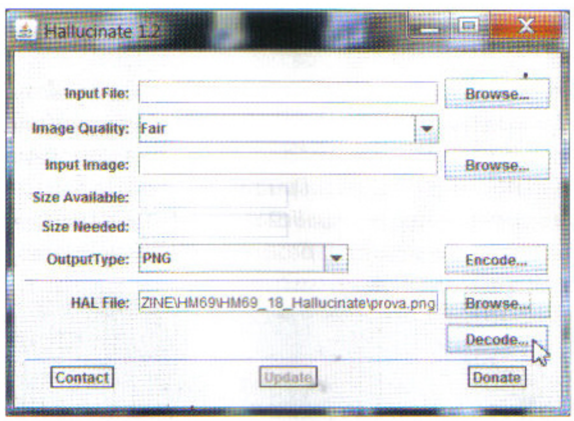
Tra le tante soluzioni per proteggere file e dati sensibili, una molto scenografica ed efficace ce la fornisce questo programma facilissimo da usare, creato da Scott Coulson. Come dice il nome stesso, Hallucinate crea un'allucinazione. Si tratta infatti di nascondere il file che vogliamo proteggere dentro un altro file di nessun interesse per un qualsiasi malintenzionato. Nella fattispecie stiamo parlando di un file BMP o PNG. Quindi, anche se i nostri file verranno aperti, mostreranno solo un'immagine scelta da noi.

Il procedimento peraltro è davvero semplice e veloce.

Per prima cosa, inseriamo nel campo **Input File** il documento da proteggere. Scegliamo la qualità dell'immagine in **Image Quality**, poi selezioniamo l'immagine da visualizzare in **Input Image** e l'estensione del file finale in **Output Type**. A questo punto è sufficiente cliccare sul pulsante **Encode** per salvare il file mimetizzato. Il processo di decodifica è ancora più semplice. Lanciamo Hallucinate e, nel campo **HAL File**, inseriamo il percorso del file criptato, dopodiché clicchiamo sul pulsante **Decode** per salvare dove vogliamo il file originale.



Per criptare un file dobbiamo agire nella parte superiore dell'interfaccia di Hallucinate. Qui selezioniamo il file da proteggere e il file dell'immagine che lo nasconderà.



L'operazione di decodifica del file criptato avviene agendo nella parte inferiore dell'interfaccia di Hallucinate. In questo caso basta indicare il file e cliccare sul pulsante Decode.

JAVA RUNTIME ENVIRONMENT

Hallucinate non ha bisogno di essere installato e possiamo lanciarlo direttamente dal CD. Tuttavia, per funzionare ha bisogno che nel nostro computer sia installato il Java Runtime Environment. Se non l'abbiamo, colleghiamoci all'indirizzo *www.java.com/it/download* e clicchiamo sul pulsante rosso Download gratuito di Java. Scaricato il file jre-6u26-windows-i586-iftw.exe, non dovremo fare altro che procedere alla sua installazione.

DIVIDE ET IMPERA

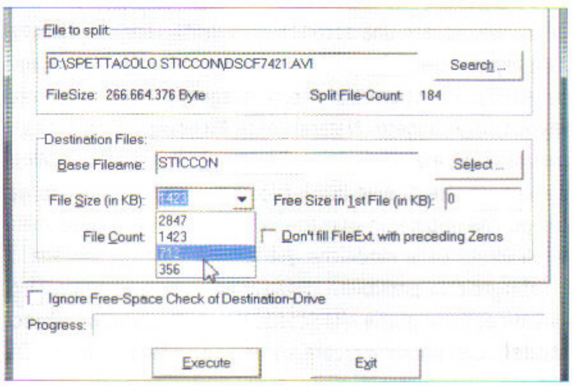
NON FACCIAMOCI PIÙ CONDIZIONARE DAI FILE DI GRANDI DIMENSIONI E GESTIAMOLI CON FILE SPLIT

di Raffaele Mazzi
redazione@hackerjournal.it

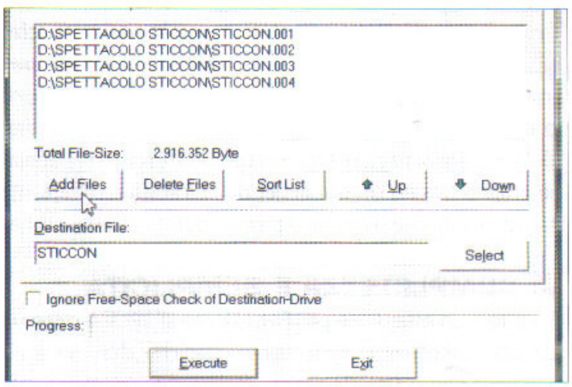
Nonostante le caselle di posta elettronica diventino sempre più grandi, così come le dimensioni dei file che possiamo allegare ai messaggi, il problema di trasferire documenti di grandi dimensioni non è ancora acqua passata. Naturalmente quello della posta elettronica è solo un esempio che però ci fa capire quanto a volte sia necessario avere a portata di mano uno strumento semplice e pratico che ci permetta di dividere i file di grandi dimensioni, per poi ricomporli quando possibile. Che sia per caricare su Usenet, per mettere su una chiavetta monumentali log di server Unix o altro ancora, ci serve uno strumento che faccia al caso nostro.

IL MINIMO INDISPENSABILE

Tra i tanti programmi in grado di suddividere un file di grandi dimensioni in documenti più piccoli, **File Split** è sicuramente uno dei migliori. Tanto per cominciare è **freeware**, quindi potremo usarlo senza limiti di tempo, né di funzioni. Inoltre ha un'interfaccia semplice, quasi spartana, che ci facilita la vita. In pratica, il programma è diviso in due cartelle (**Split** e **Concat**) e non ha alcun menu di configurazione, quindi tutte le operazioni consentite si fanno attraverso queste due finestre diverse. La prima serve per selezionare e suddividere il file, la seconda per ricomporlo. In **Split**, dovremo scrivere il percorso del file da dividere nel campo **File to split** (o usare il pulsante **Search** per fare prima), poi scriveremo il nome generico dei frammenti nel campo **Base Fileame** (sic!). Quindi dovremo indicare le dimensioni massime di ogni singolo frammento in **File Size** e cliccare su **Execute** per procedere alla suddivisione. Anche la ricostruzione del file è piuttosto semplice. Nella scheda **Concat** dovremo cliccare sul pulsante **Add Files** e selezionare tutti i frammenti, per poi cliccare su **Apri**. Se per caso i file non venissero importati in ordine, niente paura, clicchiamo sul pulsante **Sort List** e tutto tornerà a posto. Nel campo **Destination File** dovremo indicare il nome del file che verrà creato, quindi clicckeremo su **Execute** per riavere il nostro file originale.



*Nella scheda **Split**, ci sono tutti gli strumenti necessari per selezionare il file da dividere e per stabilire in KB le dimensioni massime di ciascun frammento.*



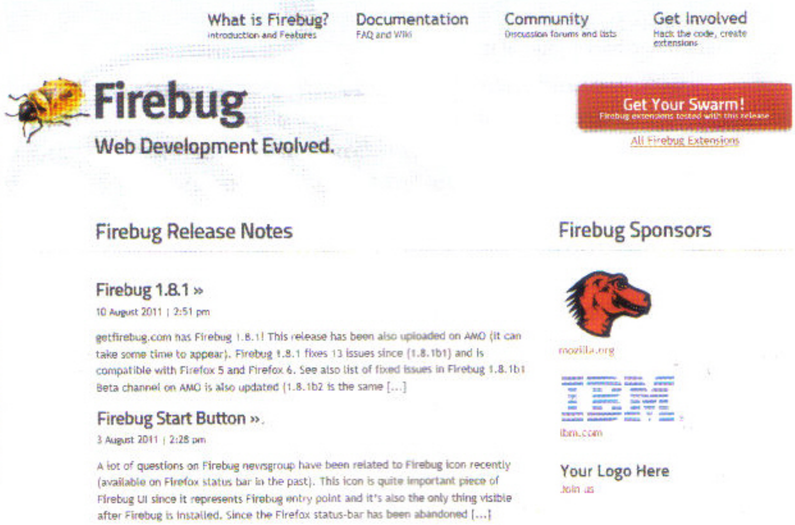
*Nella scheda **Concat** importeremo i frammenti del file che abbiamo suddiviso per riunirli in un nuovo file. Grazie ai pulsanti **Up** e **Down** potremo mettere in ordine manualmente i vari frammenti.*

UNA MARCIA IN PIÙ

Per ricomporre un intero file suddiviso in tanti frammenti File Split si semplifica la vita. Infatti, al termine della suddivisione, il programma genera il file rejoin.bat che serve proprio a ricreare il file originale. Salviamo questo file nella stessa cartella in cui ci sono tutti i frammenti a cui fa riferimento per poterlo poi lanciare e rimettere insieme i vari segmenti.

LE MANI SUI CODICI

TUTTO PER ANALIZZARE E MODIFICARE I CODICI HTML, CSS E JAVASCRIPT DEI SITI WEB E CONTROLLARE IN TEMPO REALE TUTTO QUANTO AVVIENE DURANTE UN COLLEGAMENTO. FIREBUG È IL COLTELLINO SVIZZERO PER GLI HACKER ALLE PRIME ARMI

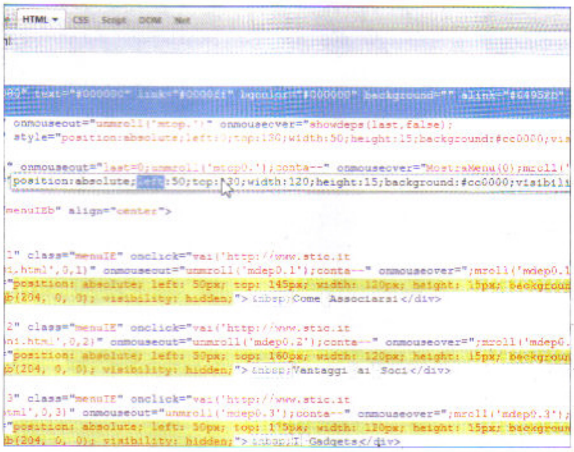


di redazione@hackerjournal.it

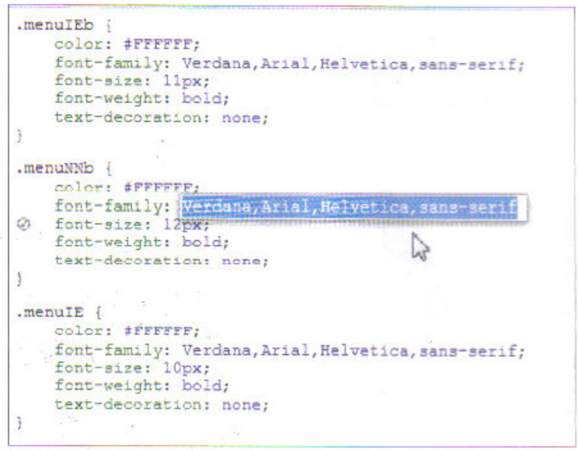
Non ha importanza se creiamo siti Web per diletto o per lavoro, ciò che ci serve è uno strumento efficace per analizzare i vari codici presenti e per correggerli in modo pratico. Se poi questo programma è anche semplice da usare, senza penalizzare la completezza, allora abbiamo proprio trovato ciò che fa per noi. **Firebug** è certamente uno strumento che risponde a pieno a queste caratteristiche.

COMPLETEZZA E SEMPLICITÀ

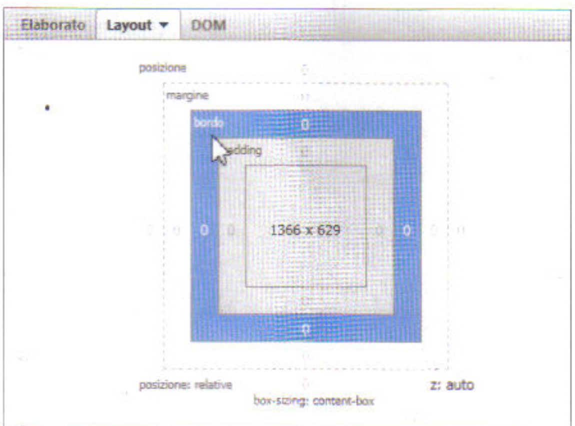
Firebug è un'estensione per **Firefox** che si installa come un qualsiasi componente aggiuntivo. Dopodiché abbiamo a disposizione uno strumento capace di darci una mano notevole nelle varie operazioni di controllo e di correzione dei codici dei nostri siti **Web**. Infatti è il **plugin** più usato per questo scopo. Della sua praticità ce ne accorgiamo fin dal primo avvio, perché ci troviamo di fronte a un'interfaccia molto ben concepita. In alto abbiamo le 6 schede tematiche (**HTML**, **CSS**, **Script**, ecc.) che ci consentono la visualizzazione di quel particolare codice o funzione del nostro sito. Inoltre, ognuna di queste schede integra il proprio menu delle opzioni, così da poter modificare i parametri di analisi mentre stiamo lavorando al suo interno. Per esempio, tramite il menu della scheda **HTML** possiamo nascondere o visualizzare i **commenti** o le **entità fondamentali** presenti nella struttura ad albero del sito, che viene mostrata nell'area principale dell'interfaccia, posta immediatamente sotto le schede. In certi casi, a destra dell'area principale, appare una seconda area in cui vengono visualizzate alcune specifiche. Nel caso della scheda **HTML** abbiamo per esempio lo strumento che ci fa agire in modo veloce sul **layout** degli oggetti. Naturalmente **Firebug** non si limita a mostrarci gli elementi che compongono il nostro sito **Web**, ma ci permette di modificarli cliccandoci sopra e agendo nel campo che appare. In questo modo vediamo immediatamente gli effetti delle modifiche. Tra le caratteristiche vincenti di **Firebug** c'è la possibilità di fare modifiche alla struttura di ciascun oggetto grazie alla scheda **DOM** (**Document Object Model**), così potremo creare anche pagine **Web** animate. Oltretutto, i cambiamenti degli attributi degli oggetti possono essere fatti senza per forza conoscere il codice **JavaScript**. **Firebug** risulta utilissimo anche nel controllo delle attività del nostro sito, quando è online. In questo caso ci viene in aiuto la scheda **Net**, che visualizza in tempo reale le richieste e le risposte effettuate. Grazie a questo strumento, oltre ad analizzare i tempi, i codici **HTTP** e i contenuti delle richieste e delle risposte, riusciremo a trovare velocemente eventuali errori presenti nelle nostre pagine per poterli correggere al volo. In fine, oltre al praticissimo **debugger** per il codice **JavaScript**, **Firebug** ha anche la funzione **profiler** che ci mostra quando vengono richiamate funzioni **JavaScript** e i tempi che impiegano a essere eseguite. Così potremo fare le modifiche necessarie per rendere il nostro sito sempre più veloce.



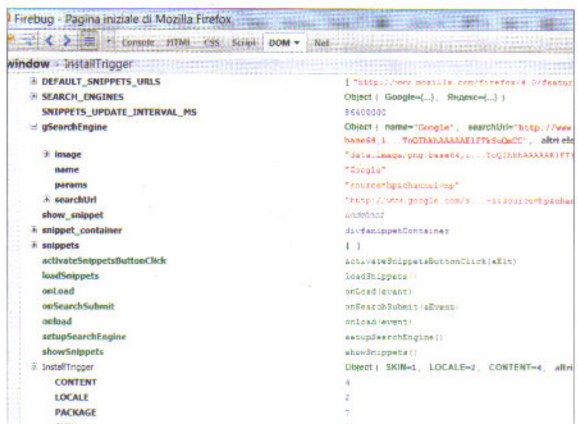
La funzione di analisi e di modifica del codice **HTML** è molto semplice. Dopo avere aperto la pagina **Web**, clicchiamo sulla scheda **HTML** ed eventualmente attiviamo/disattiviamo le opzioni nel menu a tendina, poi clicchiamo su una parte del codice e modifichiamola direttamente.



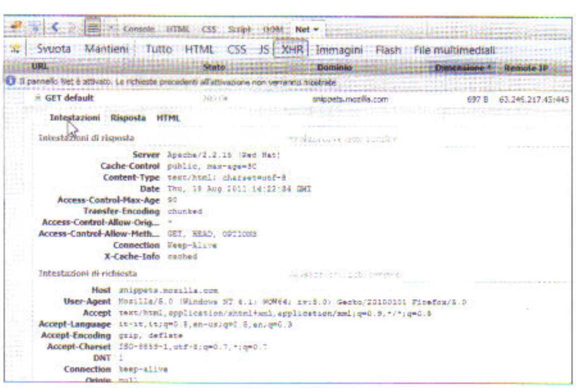
L'analisi e la correzione dei fogli di stile **CSS**, associati alla pagina **Web**, si fanno in modo simile a quanto abbiamo apena visto per il codice **HTML**. In questo caso, clicchiamo sulla scheda **CSS** e, nella schermata che appare, clicchiamo sulle righe da correggere, quindi inseriamo direttamente la correzione.



Per analizzare e modificare le dimensioni del **box** di un determinato oggetto, clicchiamo sulla scheda **HTML** e nell'area a destra, clicchiamo su **Layout**. Faremo così apparire uno strumento che ci permette di intervenire su elementi come la posizione, il margine, il bordo, ecc.



Per l'analisi del **Document Object Model** e le sue eventuali modifiche, clicchiamo sulla scheda **DOM**. Grazie a **Firebug** non è necessario conoscere **JavaScript** per fare i cambiamenti agli attributi della pagina. Nel menu a tendina della scheda **DOM** troviamo tutte le ozpioni di visualizzazione.



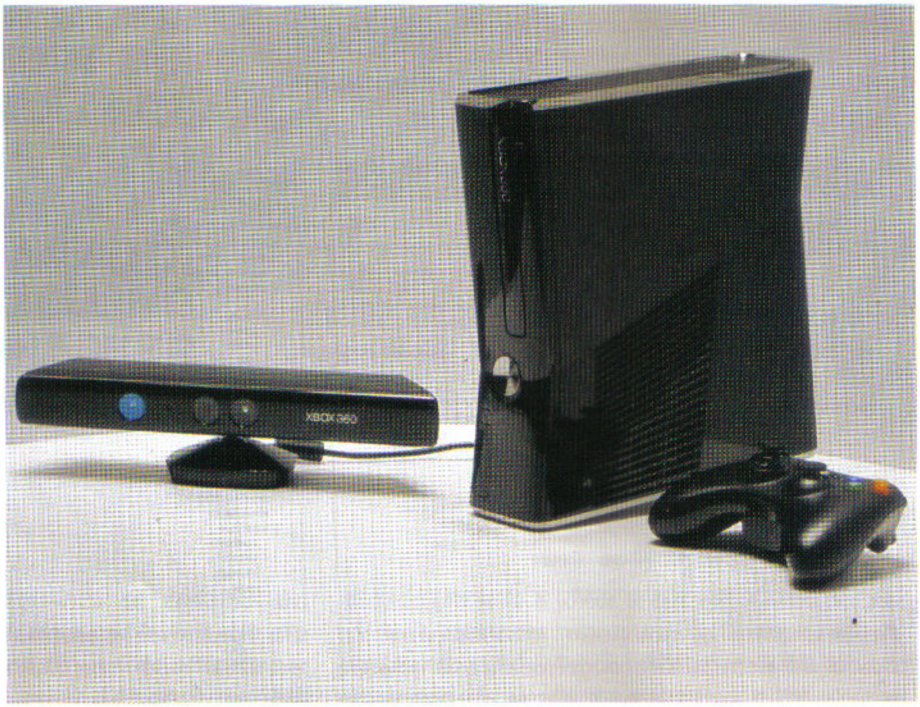
Se abbiamo bisogno di monitorare le chiamate dal sito, clicchiamo sulla scheda **Net**. Per non fare confusione, usiamo i filtri disponibili (**HTML, CSS, XHR**, ecc.) per visualizzare solo le chiamate di un certo tipo. Per ogni richiesta possiamo analizzare diversi parametri, tra cui i tempi di risposta.



Firebug ha tutti gli strumenti necessari per fare un efficace **debug** del codice **JavaScript**. Per esempio possiamo creare dei punti di interruzione dell'esecuzione del codice e inserire delle condizioni di arresto, cliccando con il pulsante destro del mouse su uno dei punti di interruzione creati.

HACKERIAMO KINECT!

SFRUTTIAMO LE DOTI STRAORDINARIE DI KINECT PER DARE SFOGO ALLA NOSTRA FANTASIA E INVENTARCI GLI HACKING PIÙ ORIGINALI, STRAVAGANTI O UTILI!

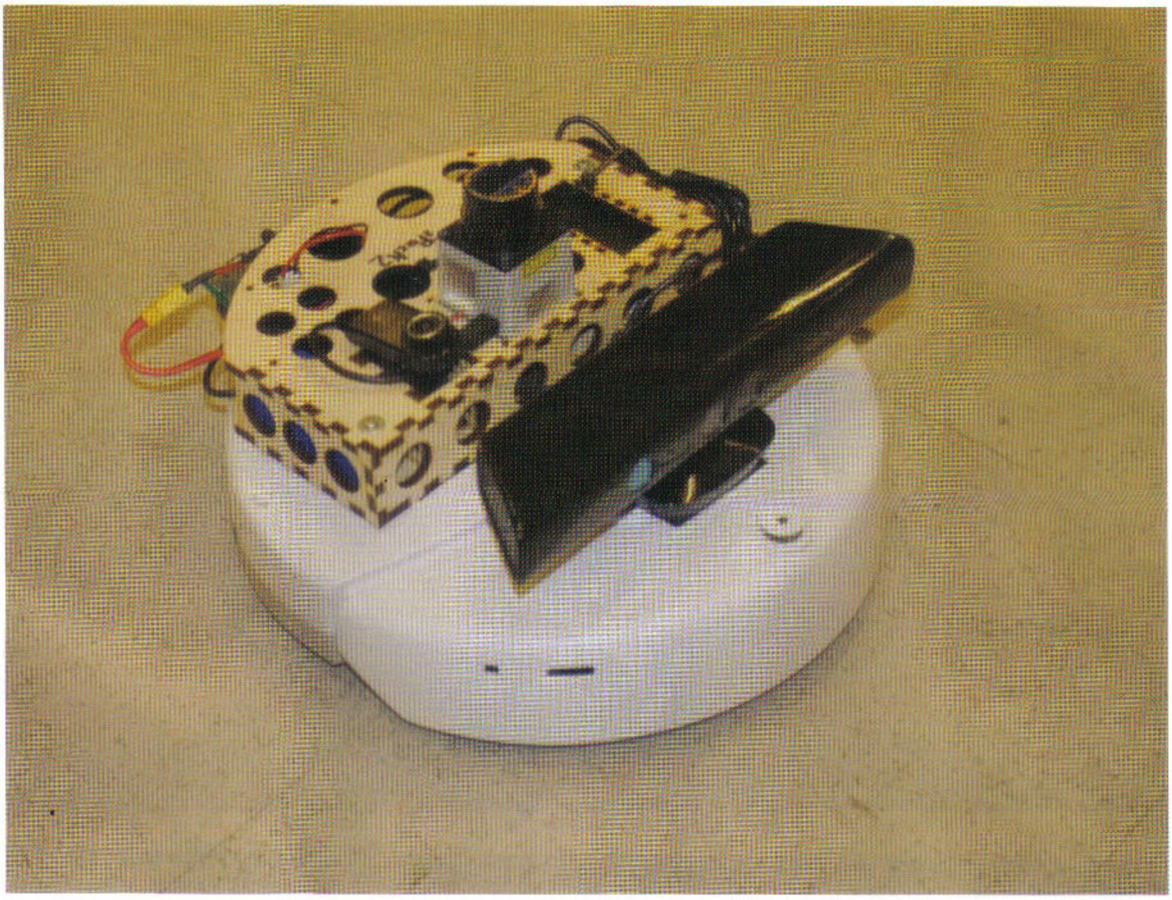


di Luca Facci
redazione@hakerjournal.it

La richiesta di una sempre maggiore interattività per le console da gioco ha spinto Microsoft a creare questa straordinaria periferica per XBox, che va oltre quanto già realizzato da Nintendo con la Wii, trasformando gli stessi utenti in controller. Di fronte a uno strumento come **Kinect**, un hacker non può fare a meno di chiedersi cosa può escogitare per andare al di là dei programmi preconfezionati e dargli nuove prospettive. E sorprendetemente questa volta è Microsoft stessa a venirci incontro con la distribuzione di un kit pensato proprio per chi vuole sviluppare applicazioni alternative con Kinect. Ecco quindi una serie di idee, tra il folle e il geniale, venute ad altri hacker, che potranno in qualche modo ispirarci. Prima però installiamo **CL-NUI-Platform** nel nostro computer, come descritto nel box a pagina 25.

SPECCHIO MAGICO

Cominciamo questa rassegna con un hacking tanto inutile quanto divertente. L'idea è venuta a **Tobias Blum** del **Politecnico di Monaco**, che sicuramente si è ispirato al fatto che **Kinect** memorizzi uno "scheletro" virtuale del nostro corpo in modo da poterne identificare più facilmente i movimenti. Ebbene, con **Magic Mirror**, così si chiama questo hacking, sullo schermo del computer viene mostrata la persona che si trova davanti alla telecamera di



Ecco come appare la creatura cibernetica di Philipp Robbel, nata dall'unione di Kinect con un iRobot Create, capace di ubbidire ai nostri comandi gestuali e di riconoscere l'ambiente.

Kinect, con un parte del corpo sostituita da una specie di radiografia ai raggi X. Quando il soggetto si muove, nella radiografia appare la parte di scheletro inquadrata. Naturalmente non si tratta di una vera e propria radiografia, ma di un effetto speciale molto riuscito, definito anche realtà aumentata, ottenuto unendo le caratteristiche di **Kinect** a uno scheletro 3D creato in computer grafica. Il video completo di questo hacking è disponibile all'indirizzo *http://www.youtube.com/watch?v=Zw_6o7AuBzk*.

IL KINECTBOT

A prima vista, la creatura di **Philipp Robbel**, uno studente del **Massachusetts Institute of Technology** negli Stati Uniti può sembrare un semplice esercizio di stile. Invece il **KinectBot**, così è stata chiamata, potrebbe avere anche applicazioni pratiche. In sostanza, **Robbel** ha unito un **iRobot Create** (una base robotizzata semovente) al **Kinect**. In questo modo si ottiene un apparecchio mobile, dotato di sensori 3D, capace di reagire ai nostri comandi. Inoltre, il **KinectBot** può realizzare e trasmettere a un computer, in modalità **wireless**, la mappatura dell'ambiente in cui si sta muovendo e l'eventuale presenza di persone, grazie alle sue capacità di rilevare i movimenti. Lo scopo finale di questo esperimento è di riuscire a creare una vera e propria squadra di robot da

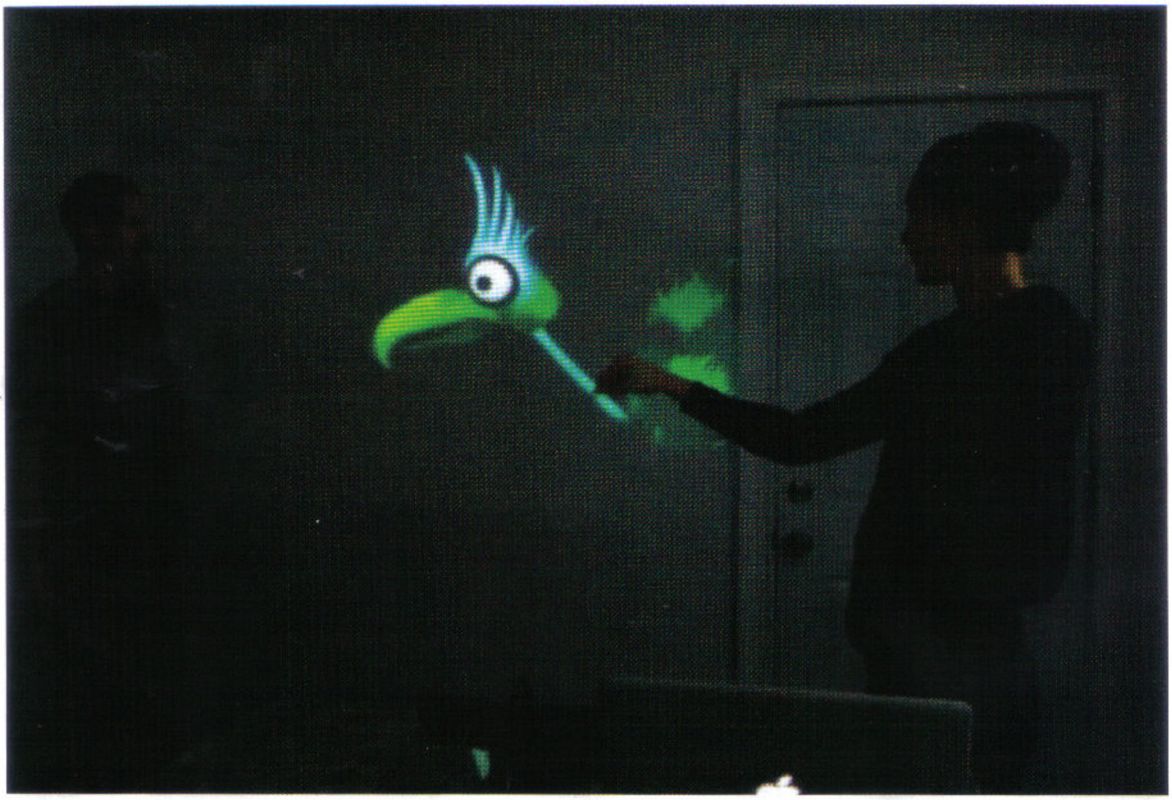
COME FUNZIONA



Kinect ha una telecamera RGB con una risoluzione di 640x480 pixel e un doppio sensore a infrarossi. Quest'ultimo è composto da un proiettore e da una telecamera (320x240 pixel) sensibile alle frequenze emesse dal proiettore. Inoltre Kinect ha un apparato microfonico che analizza i rumori dell'ambiente e serve per il riconoscimento dei comandi vocali. La barra orizzontale di Kinect è montata su un supporto motorizzato, che le consente di ruotare e di posizionarsi al meglio rispetto al giocatore, permettendo così un più preciso riconoscimento dei suoi movimenti.

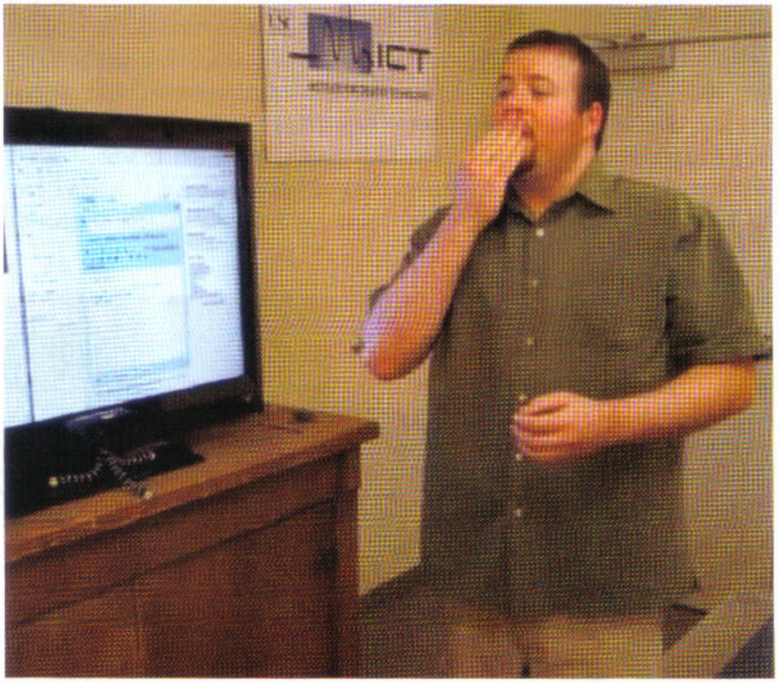
MULTIMEDIA

NEL CD



Questa immagine è tratta dal video in cui Emily Gobeille e Theo Watson danno una divertente dimostrazione del loro hacking, manovrando questo simpatico pupazzo virtuale.

impiegare in operazioni di salvataggio in ambienti particolarmente difficili o dall'accesso estremamente pericoloso, come in aree contaminate da agenti chimici o da radiazioni. Per la realizzazione del **KinectBot** sono stati impiegati, tra l'altro, alcuni pacchetti per la visualizzazione, di **Mobile Robot Programming Toolkit** (*http://www.mrpt.org*) e **GMapping** di **OpenSLAM.org**.



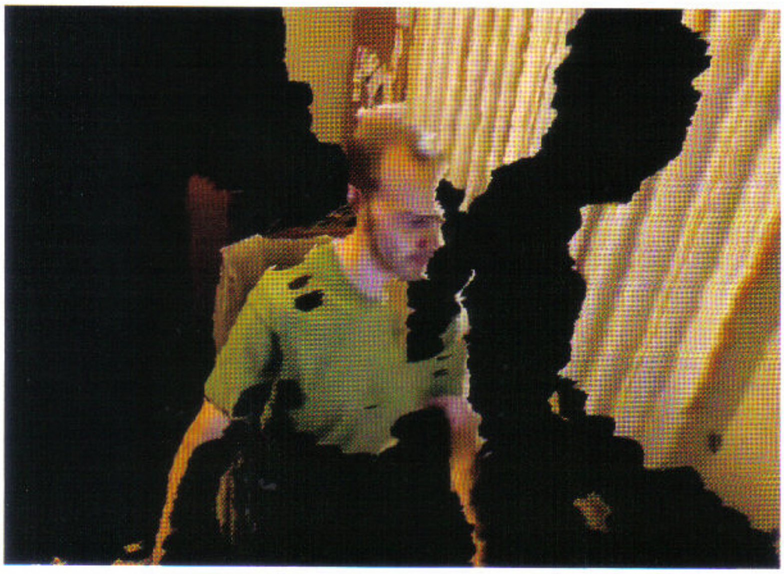
Questo studente dell'USC sta leccando il francobollo virtuale con cui affrancare l'e-mail. Con questo gesto si spedisce il messaggio di posta elettronica nell'esperimento che ha reso reale il pesce d'aprile di Gmail Motion.

BURATTINI VIRTUALI

La realizzazione di questo esperimento è la diretta conseguenza della pubblicazione di diversi **driver OpenSource**. Nel nostro caso, **Emily Gobeille** e **Theo Watson** hanno fatto buon uso dei **driver libfreenect** e di **openFrameworks** e lo dimostrano nel video che troviamo all'indirizzo *http://vimeo.com/16985224*. Il risultato finale è la creazione di un burattino tridimensionale che segue alla perfezioni i movimenti del braccio di chi lo manovra. Ovviamente dietro tutto questo c'è sempre **Kinect**, che si occupa di ricreare una sorta di scheletro del nostro arto, abbinandone poi le azioni al burattino virtuale. La precisione è davvero stupefacente, soprattutto se si osserva il becco dell'uccello, i cui movimenti sono ottenuti con quelli delle dita del burattinaio.

GMAIL MOTION

Lo scorso primo aprile, **Google** ha voluto farci il classico "pesce", parlando di una finta applicazione chiamata **Gmail Motion** che avrebbe permesso di controllare la posta coi gesti. Ebbene, nel giro di una settimana, alcuni studenti della facoltà di **Tecnologie Creative** dell'**Università della California del Sud** (**USC**) hanno trasformato lo scherzo in realtà, usando ovviamente **Kinect**. Nel video su **YouTube** (*www.youtube.com/watch?v=Lfso7_*



In questo video publicato su YouTube da Oliver Kreylos, il giovane scienziato dimostra come, usando Kinect con un software adeguato, sia possibile creare un vero effetto tridimensionale.

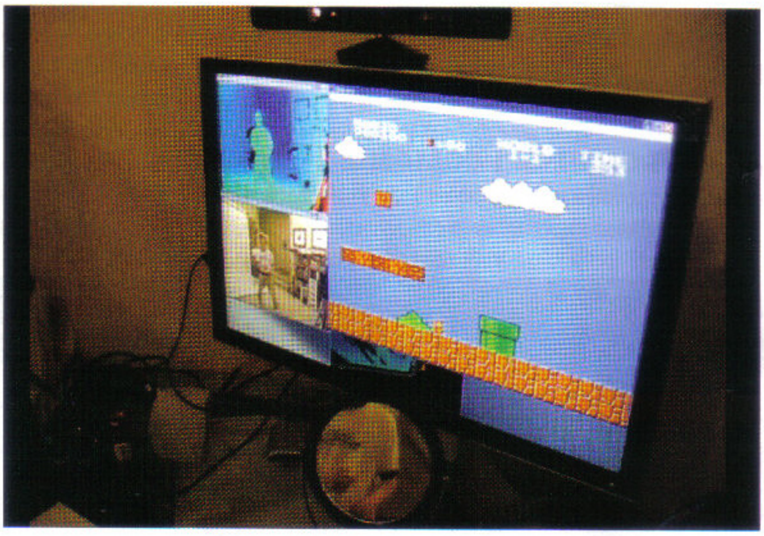
i9Ko8) **Evan Suma**, uno degli artefici di questo hacking, fa una dimostrazione pratica del suo funzionamento, basato esclusivamente sui gesti. Per esempio, vediamo come aprire un messaggio di posta elettronica e come rispondere. Il comando più bizzarro è quello di spedizione, poiché dobbiamo portare le dita alla bocca (come se leccassimo un francobollo) e poi batterle sulla coscia, per "affrancare" il messaggio!

EFFETTO 3D

C'è una sostanziale differenza tra le telecamere stereoscopiche e quelle 3D. Le prime sfruttano lo stesso principio dei nostri occhi, sovrapponendo due immagini bidimensionali leggermente sfalsate. Invece, le vere videocamere 3D ricostruiscono i frammenti dell'immagine che mancano per un completo effetto tridimensionale. Non solo calcolano i colori, ma anche le distanze tra i vari punti. Partendo dal fatto che **Kinect** possiede una vera e propria telecamera 3D, il giovane **Oliver Kreylos** è riuscito a realizzare un programma in grado di manipolare l'immagine ripresa dalla periferica di **Microsoft** per ruotarla a piacere in qualsiasi direzione per vedere una rappresentazione tridimensionale delle riprese. Lo si vede chiaramente nel video pubblicato su **YouTube** (*www.youtube.com/watch?v=7QrnwoO1-8A*). Tutto questo si è tradotto in un interessantissimo pacchetto di sviluppo per la realtà virtuale, chiamato **Vrui VR Toolkit**.

TUTTI IDRAULICI

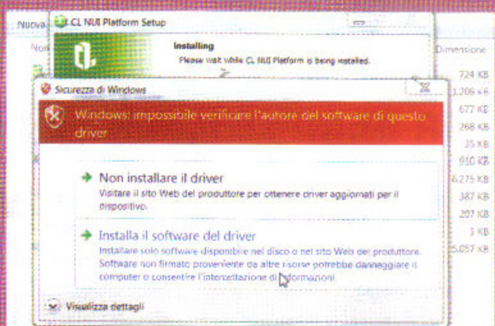
Kinect nasce soprattutto per permetterci di videogiocare in modo diverso. Quindi pare un po' banale hackerare la periferica a questo scopo. Tuttavia, come vediamo nel divertente video pubblicato sul Web all'indirizzo *www.youtube.com/watch?v=8CTJL5lUjHg*, i risultati possono essere molto interessanti, soprattutto se vengono applicati a videogiochi storici come **Super Mario Bros**: è ora di correre e saltare!



Le applicazioni degli hacking di Kinect ai videogiochi possono essere davvero tante. Eccone un esempio con il famosissimo Super Mario Bros, che possiamo ammirare su YouTube.

COLLEGHIAMO KINECT AL PC

Una delle operazioni fondamentali per potere hackerare Kinect è di collegarlo al nostro computer. Per farlo, usiamo il programma CL-NUI-Platform (solo per Windows 7), che troviamo nella sezione Hacking del nostro CD. Durante la sua installazione, appariranno un paio di finestre di avviso in cui il sistema operativo ci dice che l'autore non è sicuro. Ignoriamole e arriviamo in fondo all'installazione completa. Poi avviamo il programma e colleghiamo Kinect al nostro computer. A questo punto potremo usarlo come se avessimo una XBox!



MASTER PASSWORD

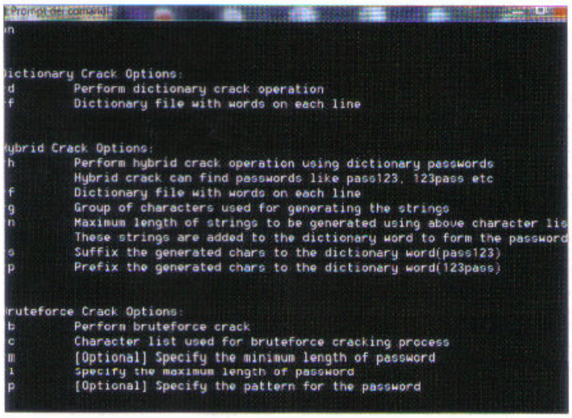
RECUPERIAMO LA PASSWORD PRINCIPALE DI FIREFOX CON FIREMASTER

di Raffaele Malazzi
redazione@hackerjournal.it

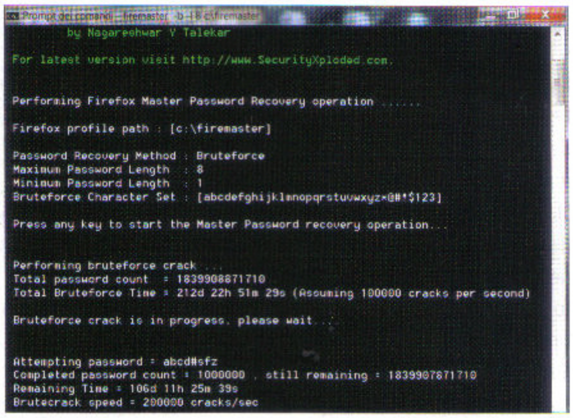
Come sappiamo, Firefox ci permette di salvare le credenziali d'accesso a un sito (nome utente e password) in modo tale da non doverle più ridigitare ogni volta. Inoltre, Firefox ci permette di creare una password (chiamata master password o password principale) per proteggere questi dati sensibili. Quindi, se la dimenticassimo, non potremmo più accedere automaticamente ai siti protetti. Siccome il salvataggio delle credenziali si fa per non dovere ricordare nome utente e password dei siti che ce le richiedono, saremmo in un gran bel guaio.

IL PROMPT DEI COMANDI

FireMaster è un utilissimo programma che ci permette di recuperare la password principale di Firefox dimenticata. Per farlo dovremo però fare uso del Prompt dei comandi di Windows. Infatti, dopo aver installato il programma, dovremo aprire proprio quella finestra, entrare nella cartella Firemaster e lanciarlo con il comando "firemaster". Così apparirà l'elenco con tutti i comandi del programma.
Tre sono i metodi di recupero della password: **Brute Force**, **Dictionary** e **Hybrid**. Il primo, che si attiva con il comando **-b**, cerca in base alla combinazione di tutti i possibili caratteri conosciuti, quindi è quello che impiega più tempo. Il secondo (comando **-d**) usa invece un file dizionario con le parole separate una per riga. È il metodo più veloce. Il terzo invece è un misto dei primi due e si attiva con il comando **-h**. Oltre ai comandi principali, dovremo inserire comandi secondari. Per esempio, dopo **-b** (**Brute Force**) dovremo inserire nella stessa riga il comando **-l** e poi indicare con un numero la lunghezza massima della password da cercare.



Dopo aver lanciato FireMaster dal Prompt dei comandi di Windows, appare questa schermata in cui ci vengono elencati per metodo di recupero i comandi da usare.



Se inseriamo il comando "firemaster -b -l 8 c:\nomecartella", il programma cercherà di recuperare una master password di 8 caratteri di lunghezza massima nella cartella indicata.

PER SEMPLIFICARCI LA VITA

Siccome la master password di Firefox viene salvata nel file key3.db, che si trova nella cartella contenuta in Profiles di Mozilla Firefox, che a sua volta si trova nella sottocartella Roaming di AppData, dentro a quella con il nostro nome utente, copiamo e incolliamo questo file altrove (per esempio nella cartella di FireMaster). Così nel Prompt dei comandi dovremo solo scrivere "c:\firemaster" e non tutto il percorso per arrivare alla cartella contenuta in Profiles di Firefox.

CARTELLE INVIOLABILI

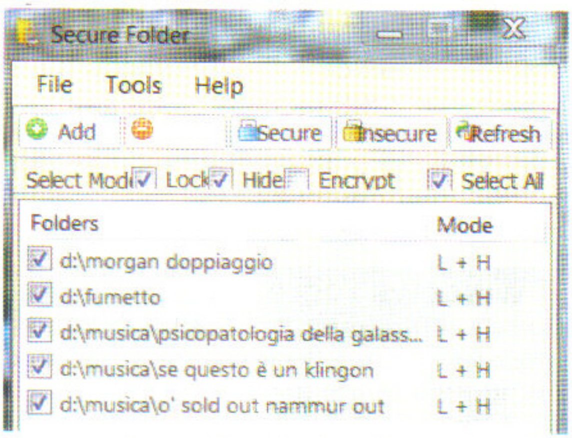
NASCONDIAMO, CIFRIAMO E BLOCCHIAMO TUTTE LE CARTELLE CHE CONTENGONO DATI PREZIOSI

di redazione@hackerjournal.it

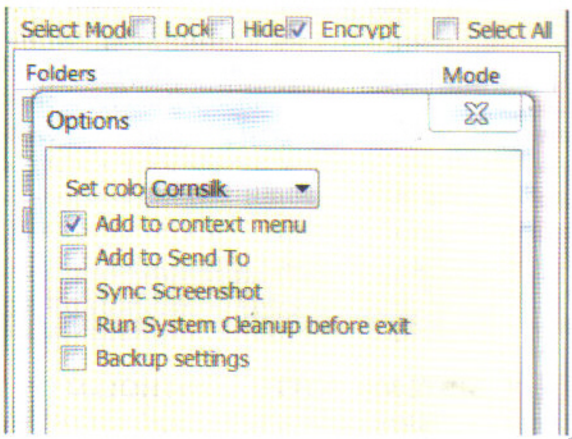
Come si dice di solito, la prudenza non è mai troppa e prima di permettere a qualcuno di mettere le mani sulle cartelle che contengono dati importanti, che non devono essere toccati, vediamo di correre ai ripari. Per farlo in modo semplice ed efficace, usiamo Secure Folder, un programma molto potente che non solo ci permette di impedire l'accesso a una cartella o la sua cancellazione, ma che può renderla invisibile.

UNA PROCEDURA SEMPLICISSIMA

Quando avviamo per la prima volta Secure Folder, una finestra ci avverte che la password predefinita è "password" e ci chiede se vogliamo cambiarla. Ovviamente clicchiamo su **Sì**, sostituiamola e clicchiamo su **Set** per confermarla. Quando viene visualizzata l'interfaccia di Secure Folder, clicchiamo su **Add** per aggiungere una cartella e ripetiamo l'operazione fino ad avere in elenco tutte le cartelle che abbiamo intenzione di proteggere. Se abbiamo deciso che tutte avranno lo stesso tipo di protezione, per esempio **Lock**, cioè bloccate, mettiamo il segno di spunta accanto a **Select All** e tutte verranno selezionate. Poi mettiamo il segno di spunta solo accanto a **Lock**, quindi clicchiamo su **Secure** per permettere al programma di agire. Se ora proviamo ad aprire una cartella bloccata, vedremo che non si può fare. Per sbloccarla, dobbiamo riavviare Secure Folder, inserendo la nostra password, poi dobbiamo selezionarla nell'elenco, quindi cliccare sul pulsante **Unsecure**. Se invece vogliamo cifrare il contenuto di una cartella, selezioniamola poi mettiamo il segno di spunta accanto a **Encrypt**, quindi clicchiamo ancora sul pulsante **Secure**. Anche se si potrà accedere alla cartella, i file contenuti avranno estensione .xxx e non potranno essere aperti. Per nascondere la cartella, dovremo invece mettere il segno di spunta accanto al comando **Hide** e procedere come visto.



Come vediamo, l'interfaccia di Secure Folder è semplicissima. In alto ci sono i pulsanti per proteggere le cartelle e sotto le modalità di protezione, quindi l'elenco delle cartelle.



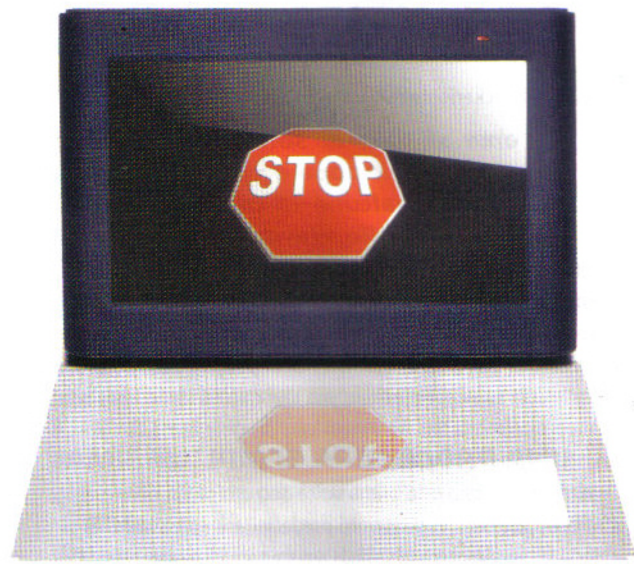
Nel menu Tools possiamo visualizzare le opzioni (Options). In questa finestra possiamo per esempio aggiungere Secure Folder al menu contestuale Invia a (Add to Send to).

MOLTI PREGI, UN DIFETTO

Diciamolo subito, Secure Folder non cripta i file compressi. Quindi se ne abbiamo, tanto vale bloccare e/o nascondere la cartella che li contiene. A parte questo, il programma ci riserva qualche ulteriore buona sorpresa nel menu Tools. Qui infatti troviamo un comando per nascondere un intero disco fisso. Inoltre con Privacy Sweep possiamo per esempio ripulire definitivamente la cartella Temp e quella del Cestino. Inoltre ci permette di cancellare definitivamente un singolo file, trascinandolo nella scheda Secure Delete.

FERMIAMO GLI INVASORI

INSTALLIAMO E USIAMO HIJACK HUNTER PER TENERE SOTTO CONTROLLO I POSSIBILI ATTACCHI CHE PUÒ SUBIRE IL NOSTRO COMPUTER E PER GESTIRE ALTRI PARAMETRI DEL SISTEMA OPERATIVO



di Francesco Barota
redazione@hackerjournal.it

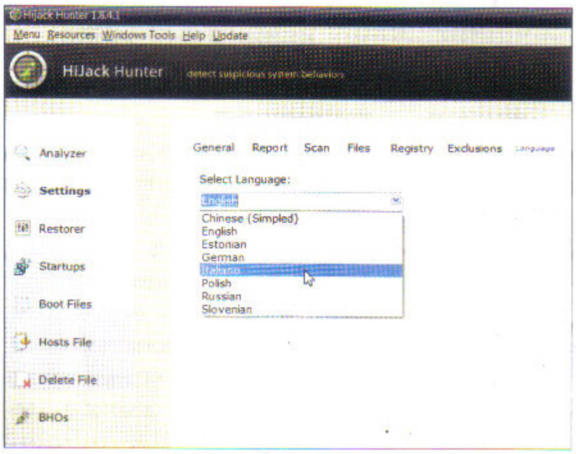
Ci sono molti indizi che possono farci sospettare che il nostro computer sia sotto attacco, come la spedizione involontaria di e-mail o il malfunzionamento ingiustificato di certi programmi. In questi casi, la prima cosa che ci viene in mente di fare è un'analisi approfondita con il nostro antivirus. Naturalmente si tratta di un'operazione più che mai corretta, che spesso porta alla soluzione definitiva del problema. Purtroppo però non sempre è così ed è proprio in questi casi estremi che entra in campo **HiJack Hunter** con tutta la sua potenza.

IL SISTEMA SOTTO CONTROLLO

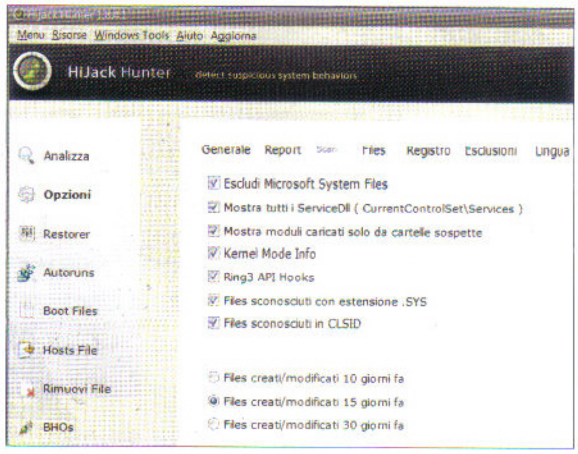
La potenza di **HiJack Hunter** si basa su alcuni suoi elementi fondamentali. Oltre al fatto che è in buona parte localizzato in italiano, quindi più immediato di altri programmi, notiamo subito la semplicità dell'interfaccia, con una barra laterale divisa per temi. Cliccando su di essi, facciamo apparire sulla destra una schermata a volte suddivisa in schede. Così potremo accedere velocemente a tutte le funzioni principali di **HiJack Hunter**. Facilissimo è anche il metodo di scansione del nostro computer. Infatti, come vedremo nella guida qui a fianco, a parte modificare alcuni parametri in base alle nostre esigenze, non dovremo far altro che cliccare sul pulsante **Scan** e al resto penserà il programma. Anche il rapporto finale risulta molto chiaro e la sua suddivisione per argomenti ci aiuta a capire velocemente dov'è il problema. Tuttavia va ricordato che i programmi di questo tipo generano un sacco di falsi positivi. Quindi, se siamo neofiti in questo tipo di operazioni, non spaventiamoci per l'elenco che sicuramente apparirà. Cerchiamo di analizzarlo con attenzione per scoprire se ci sono potenziali minacce al nostro sistema. A questo punto però dobbiamo intervenire di persona, perché **HiJack Hunter** non elimina le minacce, le segnala solamente. Tuttavia ci mette a disposizione un buon numero di strumenti per poterlo fare.

WINDOWS TOOLS

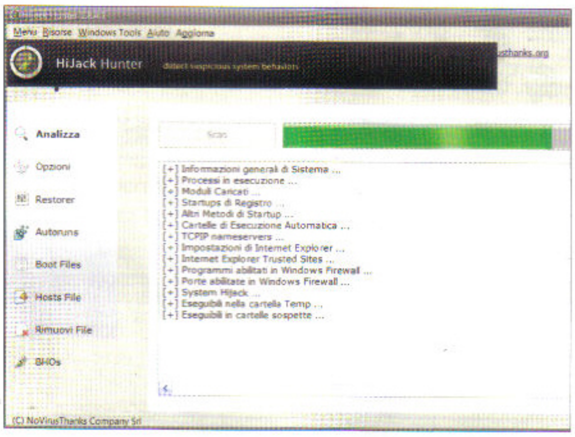
Nella barra dei menu, abbastanza minimalista, c'è una voce piuttosto ricca. Si tratta di **Windows Tools**. Aprendo questo menu, scopriamo una gran quantità di elementi. In realtà si tratta di vere e proprie scorciatoie per accedere agli strumenti di **Windows** per gestire il sistema operativo, che risultano estremamente comode. Per esempio, se vogliamo visualizzare la finestra **Gestione attività Windows**, non dovremo più premere i classici **Ctrl+Alt+Canc**, ma basterà cliccare sulla voce **Task Manager**. Un altro esempio: se vogliamo visualizzare l'**Editor del Registro di sistema**, non dovremo più scrivere il comando **regedit**, ma cliccheremo su **Registry Editor**. In questo utilissimo menu ci sono anche altri comandi che attivano in modo semplice e diretto funzioni di **Windows** senza doverle andare a cercare in lungo e in largo. Quindi, oltre a essere un'ottima sentinella che ci avverte degli attacchi al nostro computer, **HiJack Hunter** è anche un valido strumento per gestire il nostro sistema operativo.



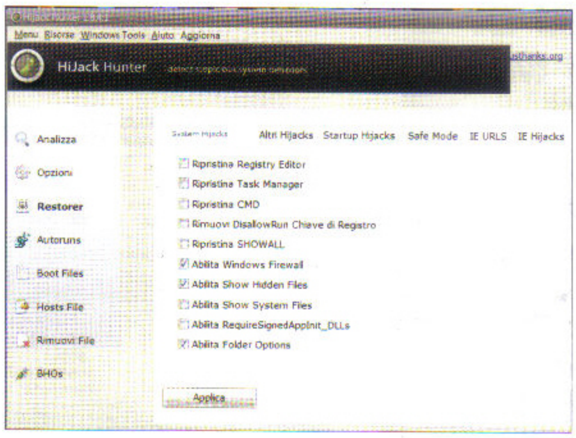
*Dopo aver avviato il programma, clicchiamo a sinistra su **Settings** e, nella scheda **Language**, selezioniamo **Italiano** dal menu a tendina. Ora apriamo la scheda **Generale** e selezioniamo/deselezioniamo le opzioni in base alle nostre necessità, per esempio **Lavora in background**.*



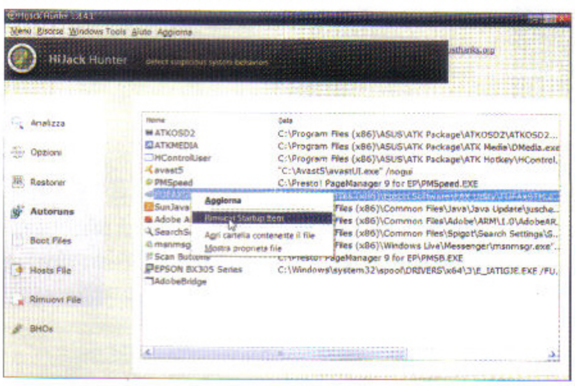
*Sempre in **Opzioni**, apriamo la scheda **Scan**. Qui possiamo decidere quali tipi di file esaminare o non esaminare. Per esempio possiamo togliere il segno di spunta da **Escludi Microsoft System Files**, oppure possiamo decidere di includere i **Files creati/modificati 10 giorni fa**.*



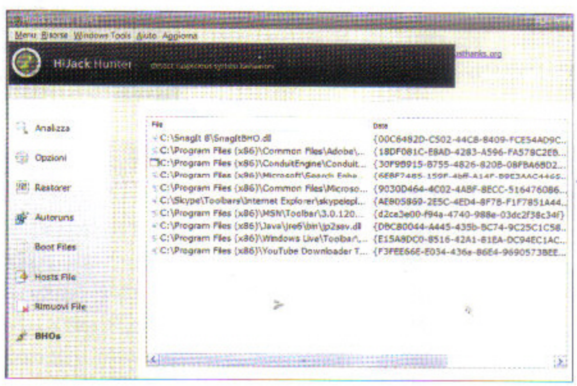
*Ora, a sinistra, clicchiamo su **Analizza** e, nella nuova schermata, clicchiamo sul pulsante **Scan** per avviare il controllo de nostro sistema. L'operazione può richiedere alcuni minuti, in base al numero di file da analizzare e alla potenza del sistema. Al termine viene mostrato un rapporto in un file **LOG**.*



*Clicchiamo su **Restorer**. Nella scheda **Sysem Hijacks**, possiamo selezionare alcune modifiche al sistema, come **Abilita Windows Firewall**. Stessa cosa possiamo fare nelle altre schede. Poi dobbiamo cliccare sul pulsante **Applica**, attendere qualche secondo, quindi riavviare il sistema.*



*Clicchiamo su **Autoruns**. Qui vediamo l'elenco dei programmi che si avviano automaticamente all'accensione del computer. Clicchiamo su uno di essi con il pulsante destro del mouse e, per esempio, selezioniamo **Rimuovi Startup Item** nel menu contestuale per impedirgli l'autoavvio.*



*In **BHOs**, vediamo l'elenco dei **Browser Helper Objects**, cioè quei programmi che si avviano quando lanciamo il programma di navigazione **Internet**. Cliccando con il destro su uno di essi possiamo vederne le informazioni ed eventualmente aprirne la cartella per disinstallarlo.*

IL TORMENTONE WEB

FOLLE E DISSACRANTE

CON PIÙ DI MEZZO MILIARDO DI POST PUBBLICATI, ECCO IL SITO PER SMANETTONI PIÙ POLITICAMENTE SCORRETTO DEL WEB CHE È ORMAI DIVENTATO UN FENOMENO DI COSTUME... O DI MALCOSTUME!



di Elio Brighi
redazione@hakerjournal.it

Si chiama 4chan (www.4chan.org), ed è uno dei siti più frequentati del Web. Le cifre parlano chiaro: più di 560 milioni di post in totale, oltre 10 milioni di visitatori al mese e circa un milione di post al giorno! Insomma, cifre da capogiro. Eppure di **4chan** non si parla molto.

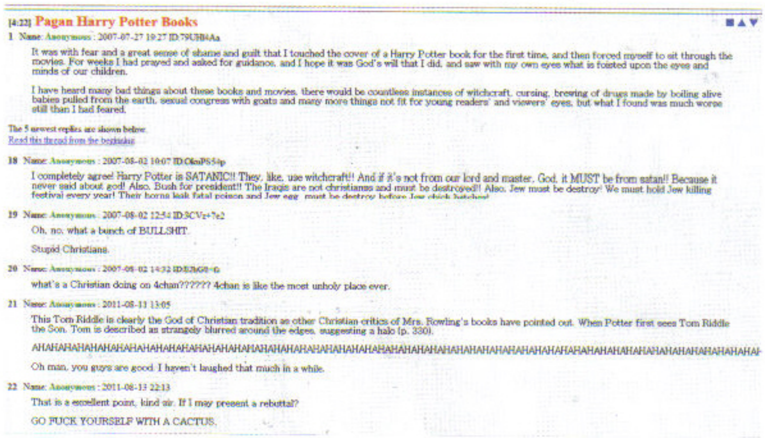
UNA FACCIA DAVVERO ANONIMA

Ma cos'è **4chan**? Tecnicamente si tratta di una delle tante **imageboard** in inglese che circolano nel **Web**, cioè un luogo in cui possiamo pubblicare immagini e commentarle. Fin qui niente di strano. Anche la veste grafica della **homepage** risulta piuttosto anonima. L'unica cosa che si fa notare è la gran quantità di argomenti di cui si occupa questo **forum**, ma neppure questa è una caratteristica unica. Eppure, questa facciata quasi rassicurante, per non dire soporifera, altro non è che l'entrata principale per l'inferno! Sì, perché non appena clicchiamo su uno dei temi, verremo catapultati nel luogo più anarchico che possiamo immaginare, dove è praticamente tutto permesso e dove la natura umana riesce a dare anche il peggio di sé.

L'ANTI-FACEBOOK

Ci sono vari modi di vivere il **Web** e sicuramente **Facebook** e **4chan** rappresentano i due estremi opposti. Il primo è una rete sociale, in cui ci presentiamo con nome e cognome, raccontando i fatti nostri a tutto spiano. Il secondo invece potrebbe essere definito **rete asociale,** dove l'anonimato

regna sovrano. Infatti su **4chan** possiamo inserire qualsiasi tipo di post e commento, nascondendoci dietro il **nick Anonymous**. Ovviamente c'è chi considera tutto questo un modo vigliacco di vivere la **Rete**. Eppure, potrebbe non essere del tutto vero. Infatti non dimentichiamoci che anche nel tanto democratico Occidente esistono i reati di opinione, come l'italianissimo vilipendio a certe cariche dello Stato, retaggio del periodo savoiardo! Quindi esprimere opinioni in forma anonima non è sempre un atto di vigliaccheria, ma di autotutela.



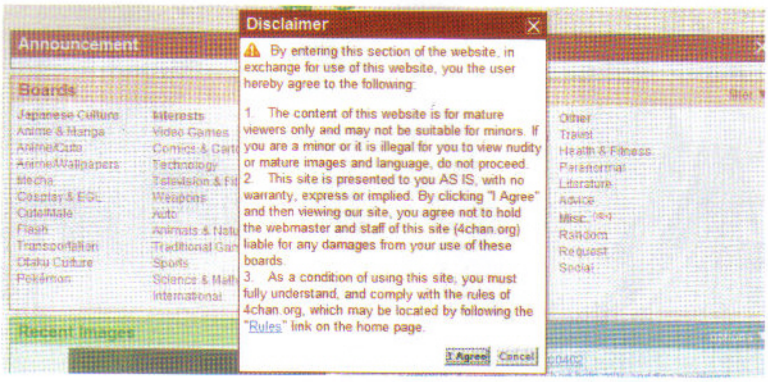
Ecco un esempio di colluttazione verbale, tipica di 4chan. Un probabile fanatico religioso si scaglia contro la saga di Harry Potter, accusandola di satanismo. Immediatamente viene sbeffeggiato e coperto di insulti da chi, evidentemente, non la pensa come lui.

IL REGNO ANARCHICO

Tuttavia, sarebbe ugualmente esagerato considerare **4chan** "l'ultima casa accogliente" di chi non può avere voce in altro modo. No, qui vige l'anarchia nel senso più ampio del termine. Qui trovano sfogo anche gli istinti più bassi e meschini dell'essere umano. Ne è un triste esempio il caso di **Jessie Slaughter** (**nick** di una ragazzina undicenne), fan dei **Blood on the Dance Floor**, una **band Emo** americana. Il filmato in cui si difendeva dalle accuse di aver avuto una relazione con il cantante della **band** venne pubblicato su **4chan** e in breve si risalì al nome e all'indirizzo della ragazzina, anch'essi pubblicati sul sito. Da quel momento, **Jessie Slaughter** venne fatta oggetto di continui attacchi personali, tanto da dovere essere messa sotto protezione dalle autorità competenti.

/B/ - RANDOM

L'episodio che abbiamo narrato ha avuto come teatro quello che viene considerato il vero e proprio "lato oscuro" di **4chan**: la famosa (o famigerata) sezione **/b/ - Random** (*http://boards.4chan.org/b*). Qui c'è proprio di tutto, di più e anche oltre! È interessante notare che proprio questa sezione genera i 2/3 dell'intero traffico del sito ed è quella in cui l'anonimato la fa da padrone assoluto. Tuttavia, a dimostrazione che **4chan** non è solo volgarità e anarchia fine a sé stessa, c'è l'episodio del gatto **Dusty**. La povera bestiola era stata sottoposta a sevizie dal padrone, che aveva orgogliosamente pubblicato le proprie malefatte su **YouTube**. Ebbene, grazie a **4chan**, il colpevole fu rintracciato e assicurato alla giustizia nel giro di 48 ore. Quindi esprimere giudizi, in un senso o nell'altro, su questo prodotto della nostra epoca risulta quanto mai azzardato, perché sarebbe come giudicare in modo univoco l'animo umano. Preferiamo comunque essere liberi di decidere se frequentarlo o no, piuttosto che qualcuno ci impedisca di farlo a suo insindacabile giudizio!



Entrare nelle sezioni 18+, cioè per adulti, non è poi così difficile. Infatti basta cliccare sul pulsante "I Agree" della finestra che appare, in cui ci viene detto di non procedere se siamo minorenni e che se procediamo lo facciamo a nostro rischio e pericolo.

LA CULLA DEI TORMENTONI

4chan è un luogo in cui si potrebbero passare mesi ad ammirare abissi e picchi dell'umanità, come abbiamo avuto modo di spiegare. Ma è anche la culla dei tormentoni, il luogo in cui nascono quasi tutte le serie di immagini satiriche che spopolano sul Web e su cui torneremo sui prossimi numeri. Dietro 4chan c'è Christopher Poole che ha creato il sito quando aveva 15 anni. Oggi il nostro eroe ne ha 23 e, nonostante l'incredibile successo della sua creatura, non è né ricco, né famoso, almeno non come Mark Zuckerberg. Anzi, a quanto pare, fino a un paio di anni fa viveva con la madre, una situazione che negli USA è tutto fuorché normale. Attulmente sta lavorando a un nuovo progetto: Canvas (*http://canv.as*), un'altra imageboard che, per il momento, è ancora in versione Beta e alla quale ci si può iscrivere tramite Facebook.

